THE CYBERSPACE DOMAIN: PATH TO A NEW SERVICE?

A Monograph

by

Colonel Eric J. Denny
United States Air Force

School of Advanced Military Studies
United States Army Command and General Staff College
Fort Leavenworth, Kansas

2013-01

Approved for Public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
		Monograph, JUN 2012-MAY 2013

4. TITLE AND SUBTITLE
The Cyberspace Domain: Path to a New Service?

5. FUNDING NUMBERS

6. AUTHOR(S)
Colonel Eric J. Denny, United States Air Force

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
School of Advanced Military Studies
201 E. Reynolds Ave.
Fort Leavenworth, KS 66027

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Command and General Staff College
1 Reynolds Ave.
Fort Leavenworth, KS 66027

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED

12b. DISTRIBUTION CODE

13. ABSTRACT ***(Maximum 200 Words)***

Cyberspace is a contested domain. Characteristics of the domain inspire a variety of actors to conduct operations in and through cyberspace. US and foreign government policy officials are focused on creating strategies and norms to reduce current risks through cyberspace to national interests. The Department of Defense has designated cyberspace a war fighting domain as a mechanism to facilitate organizing cyber forces like land, air, and sea forces. There are services with lead responsibility for the land, air, and sea domains. Does this fact suggest a separate service responsible for cyberspace will evolve? This monograph examines US cyber forces organizational constructs and explores organizational change mechanisms, environmental conditions, and actor motivations that might lead to establishment of a separate Cyber Force.

14. SUBJECT TERMS	15. NUMBER OF PAGES
Cyberspace, Organization, Motivation, Service, CYBERCOM, SOCOM	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED

MONOGRAPH APPROVAL PAGE

Name of Candidate: Colonel Eric J. Denny

Monograph Title: The Cyberspace Domain: Path to a New Service?

Approved by:

_____, Monograph Director
Robert T. Davis II, Ph.D.

_____, Second Reader
G. Scott Gorman, Ph.D.

_____, Director, School of Advanced Military Studies
Thomas C. Graves, COL

Accepted this 23rd day of May 2013 by:

_____, Director, Graduate Degree Programs
Robert F. Baumann, Ph.D.

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the US Army Command and General Staff College or any other governmental agency. (References to this study should include the foregoing statement.)

ABSTRACT

THE CYBERSPACE DOMAIN: PATH TO A NEW SERVICE? by Col Eric J. Denny, United States Air Force, 65 pages.

Cyberspace is a contested domain. Characteristics of the domain inspire a variety of actors to conduct operations in and through cyberspace. US and foreign government policy officials are focused on creating strategies and norms to reduce current risks through cyberspace to national interests. The Department of Defense has designated cyberspace a war fighting domain as a mechanism to facilitate organizing cyber forces like land, air, and sea forces. There are services with lead responsibility for the land, air, and sea domains. Does this fact suggest a separate service responsible for cyberspace will evolve? This monograph examines US cyber forces organizational constructs and explores organizational change mechanisms, environmental conditions, and actor motivations that might lead to establishment of a separate Cyber Force.

TABLE OF CONTENTS

INTRODUCTION 1

CYBERSPACE DOMAIN BACKGROUND 6

Definition of Cyberspace 6
Characteristics of Cyberspace Operations 8

CYBERSPACE OPERATIONAL ENVIRONMENT 22

A Contested Domain 22
Strategic Cyber War and Cyberspace Operations Thinking 27

OBSERVATIONS ON FORMATION OF THE AIR FORCE 35

THE POST SEPARATE SERVICE ERA? 40

Goldwater-Nichols and the New Jointness 40
SOCOM – Rise of the Service-Like COCOM 42

CYBER FORCES ORGANIZATIONAL STRUCTURE 47

US Cyber Command 47
Evolution of Cyber Force Structures 50
The Time Factor 55

MOTIVATIONS FOR ORGANIZATIONAL CHANGE 56

Personal Motivations 56
Organizational Efficiency Motivations 58

CONCLUSION 63

APPENDIX A: NETWORKING AND INTERNET HISTORY 66

APPENDIX B: REVIEW OF CYBERSPACE POLICY AND LEGISLATION 70

APPENDIX C: INTERNATIONAL EFFORTS TO ESTABLISH CYBERSPACE NORMS 80

APPENDIX D: THE ROAD TO A SEPARATE AIR FORCE 84

APPENDIX E: CYBERSPACE RESPONSIBILITIES IN THE US GOVERNMENT 93

APPENDIX F: SERVICE COMPONENT CYBER ORGANIZATIONS.....96

INTRODUCTION

Cyberspace will turn 44 years old in 2013. The word itself, cyberspace, came into being in the 1980s.[1] Military cyberspace operations date back to the 1991 Persian Gulf War.[2] The Department of Defense (DoD) declared cyberspace a war fighting domain in 2005, making it the fifth alongside land, sea, air, and space. The 2011 DoD Strategy for Operating in Cyberspace states cyberspace was declared a domain as an organizing concept necessary to organize, train, and equip cyber forces like air, land, and sea forces. [3] Air, land, and sea forces are represented by independent Service branches. This raises the question, do we need a separate Cyber Force?

This paper examines if designation of cyberspace as a war fighting domain will lead to the establishment of a separate Cyber Force. The focus of study is on the process behind significant organizational change in the US military and factors that affect the motivation of actors to seek a separate service including personal aspirations and organizational effectiveness. The paper will not address specific arguments for or against the creation of a separate Cyber Force.[4] At this time it appears that the US government's proclivity towards incremental change along with positive characteristics of the current organizational construct will undercut calls for a separate Cyber Force. The relatively short history of the current cyber forces organizational

---

[1]Attributed to science fiction author William Gibson.

[2]Richard Clarke, and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: HarperCollins, 2010).

[3]U.S. Department of Defense, *Department of Defense Strategy for Operating in Cyberspace, July 2011*, 5, http://www.defense.gov/news/d20110714cyber.pdf (accessed 15 February 2013).

[4]Publicly expressed advocacy for a separate Cyber Force does exist. For a culture based argument see Gregory Conti and John Surdu, "Army, Navy, Air Force, and Cyber—Is it Time for a Cyberwarfare Branch of Military?" *AInewsletter* 12 no. 1 (Spring 2009): 14-18, http://www.rumint.org/gregconti/publications/2009_IAN_12-1_conti-surdu.pdf (accessed 23 April 2013).

structure within DoD precludes a clear cut picture of factors that will affect motivation however, which indicates it will be useful to re-examine the question posed by this paper at least every decade. Because the record of performance of cyber organizations is short, final consideration is given to future events that could lead to a separate Cyber Force including the rise of organic cyber leaders to four-star rank within the Services and a future war in which cyberspace operations have major impact on the US.

This monograph begins with a contextual examination of cyberspace to develop understanding of the domain and then examines the organizational change process and factors that affect motivation to seek a separate Cyber Force. Section one consists of a definition of cyberspace and examination of characteristics of cyberspace which make the domain attractive for military operations. Section two explores the contested nature of cyberspace and current trends in US, Russian, and Chinese strategic thinking about cyberspace. Section three explores the organizational change process within the US Government by reviewing observations on the historical example of the Air Force. Section four explores evolution of the organizational change process after the establishment of the Air Force and how this may preclude a separate Cyber Force. Section five reviews the current cyber force structure, focusing on US Cyber Command (USCYBERCOM), created by the Secretary of Defense in 2009 and currently led by General Keith Alexander. Section four also examines the evolution of cyber forces since 2009 to identify how the force construct and timing will affect the case for a separate Cyber Force. Section six examines whether motivational factors including personal aspirations and organizational effectiveness will underpin or undercut calls for a separate Cyber Force.[5]

[5] There are six appendices included which provide expanded exploration of cyberspace and force structures for those interested in deeper exploration of the domain.

Early writing on cyberspace topics from the 1970s, exemplified by Howard Franks report for the Advanced Research Projects Agency (ARPA) and Star Roxanne Hiltz and Murray Turoff's *The Network Nation*, consist largely of technical writings on computer networking solutions and futurist musings on the social and collaborative effects cyberspace would have on society.[6] The first widely publicized warning that cyberspace was weaponizable appeared in 1990 and spurred a slew of texts throughout the 1990s addressing "information warfare" by authors such as Winn Schwartau and Heidi and Alvin Toffler.[7] Examination of cyberspace defense topics by think tanks, universities, and US Government entities also expanded at this time coincident with expanding US Policy-maker attention to cyberspace. Influential writers include Martin Libicki, Paul Rosenzweig, and James Lewis.[8] Foreign nations also paid attention to cyberspace in

---

[6]Howard Frank, "The Practical Impact of Recent Computer Advances on the Analysis and Design of Large Scale Networks," Network Analysis Corporation report prepared for Advanced Research Projects Agency, December 1973, http://www.dtic.mil/dtic/tr/fulltext/u2/777738.pdf (accessed 24 April 2013); also Starr Roxanne Hiltz and Murray Turoff, *The Network Nation: Human Communication Via Computer*, rev. ed. (Cambridge, Mass.: The MIT Press, 1993).

[7]National Research Council Staff, *Computers at Risk: Safe Computing in the Information Age* (Washington, DC: National Academies Press, 1990), 7-8, http://site.ebrary.com.lumen.cgsccarl.com/lib/carl/docDetail.action?docID=10056738 (accessed 3 February 2012); also Winn Schwartau, *Information Warfare: Chaos on the Electronic Superhighway* (Thunder's Mouth Press, May 1994); also Alvin and Heidi Toffler, *War and Anti-War* (New York: Warner Books, 1993).

[8]Martin C. Libicki and RAND Corporation, *Conquest in Cyberspace: National Security and Information Warfare* (New York: Cambridge University Press, 2007), http://carl.summon.serialssolutions.com/document/show?id=FETCHMERGED-carl_catalog_3635251&s.q=Conquest+in+Cyberspace%3A+National+Security+ and+Information+Warfare&spellcheck=true (accessed 12 September 2012); also Paul Rosenzweig, *The Alarming Trend of Cybersecurity Breaches and Failures in the US Government* (Washington DC: The Heritage Foundation, May 24, 2012) http://www.heritage.org/research/reports/2012/05/the-alarming-trend-of-cybersecurity-breaches-and-failures-in-the-us-government (accessed 24 April 2013); also James Lewis, *Cybersecurity Two Years Later: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency* (Washington, DC: Center for Strategic and International Studies, 2011).

the 1990s, with particular interest in the role of information warfare in the success of the US military invasion to liberate Kuwait. Increasing numbers of translated original texts as well as overviews such as Timothy Thomas' *Recasting the Red Star,* and Jeffrey Carr's *Inside Cyber Warfare,* are available.[9] This monograph is heavily influenced by Gregory Rattray's *Strategic Warfare in Cyberspace* due to his extensive treatment of the topic and because many of Rattray's comments or recommendations appear to be reflected in current cyberspace policy documents.[10]

In the last decade, successive iterations of cyberspace policy documents have been published and the topics covered have grown considerably in scope. A large amount of focus is recently given to cyberspace defense, cyberspace vulnerabilities, and deterrence strategy development. There is a lack of information in the open source environment on US offensive capabilities other than news article reporting on malware attributed to the US. Examination of cyberspace forces organization has been conducted by think tanks and government entities such as RAND Corporation and the Government Accountability Office. Additionally, there has been a significant increase in both commercial and military professional journal articles on cyberspace organization, threats, and policy topics in recent years. David Hollis' "USCYBERCOM: The Need for a Combatant Command versus a Subunified Command," is a particularly notable example of such writings.[11] Considerable attention has been also been given to cyberspace topics by military monographs, with topics including contextual understanding of cyberspace warfare

---

[9]Timothy Thomas, *Recasting the Red Star: Russia Forges Tradition and Technology through Toughness* (Fort Leavenworth: Foreign Military Studies Office, 2011); also Jeffrey Carr, *Inside Cyber Warfare* (Sebastopol: O'Reilly-Media, 2013)

[10]Gregory Rattray, *Strategic Warfare in Cyberspace* (Cambridge, MA: Massachusetts Institute of Technology, 2001).

[11]David M. Hollis, "USCYBERCOM: The Need for a Combatant Command Versus a Subunified Command," *Joint Forces Quarterly* 58 (3d quarter 2010): 48-54, http://www.ndu.edu/press/USCYBERCOM.html (accessed 7 April 2013).

concepts, military operations, threats, and organizational issues. Congressional testimony, newspaper articles, and leader speeches were relied on for examination of recent developments among US Government cyberspace organizations. Richard Clarke's *Cyber War: The Next Threat to National Security and What to Do About It*, is useful as an overview of cyberspace concepts and policy issues.[12]

Recently, authors such as Jeffrey Carr have used the pervasive nature of cyberspace to facilitate their research using "open source" intelligence and "crowd sourcing" techniques to explore the vast amount of information available on the Internet. Future examination will (and should) probably rely even more on cyberspace tools to conduct research. One such currently feasible (but probably economically unaffordable) example would be to harness "big data" analytics in conjunction with the "natural language" processing capabilities of IBM's Watson System to both suggest and examine cyberspace topics utilizing information quantities too large for effective human processing.

[12] Clarke and Knake, *Cyber War: The Next Threat to National Security and What to Do About It.*

CYBERSPACE DOMAIN BACKGROUND

The adjective "new" appears quite often in recently published monographs and news articles that discuss cyberspace as a warfighting domain. "New to you" or "newly declared" are more appropriate terms, however, as cyberspace and conflict within it may be young, but not new. Operations in cyberspace go back to the 1991 Persian Gulf War.[13] The US government put out the first cyberspace policy in 1998, and the Air Force added cyberspace to its mission statement in 2005. Some mission sets in cyberspace are fairly mature including: Information Operations, Electronic Warfare and to a lesser extent Network Attack.[14] The likely reason so many observers are inclined to use the word "new" is because either elements of the current cyberspace have gone by various other names over the last two decades or else they have not been paying attention to the domain until recently. The following section begins with the definition of cyberspace and then examines characteristics of operations in cyberspace in order to develop understanding of the domain before exploring the current cyberspace operating environment.[15]

Definition of Cyberspace

Cyberspace is defined by DoD as "A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems and embedded processors and

---

[13]Clarke and Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, 34.

[14] Cyberspace and Information Operations (IO) appear to be diverging in some sense as the 2012 Unified Command Plan transferred responsibility for IO from USSTRATCOM to the Joint Staff.

[15] See Appendix A for a review of the history of computer networking and the Internet.

controllers."[16] Embedded in the short definition of cyberspace are several complex concepts which foster confusion if one has not previously spent time thinking about the topic. Information can be transmitted between users in analog or digital form; as differentials of electrical signals over wires or photons in fiber optic cables, or as amplitude or frequency modulation patterns of electromagnetic waves between a variety of transmitter and receiver types including radios, satellites, microwave antennas, cellular antennas, etc. The Internet (as well as telecommunication systems) consists of physical structures as well as protocol standards. It is accessed via cabled or electromagnetic wave connections (wireless), through telephone, satellite, cable, cellular, or radio systems. Information is transmitted in forms defined by established protocols and facilitated by software programs written for laypersons. Computer systems come in ever expanding varieties including smart phones, tablets, laptops, PCs, and servers. Embedded processors and controllers are present in computers, environmental support systems, traffic systems, electrical grid control systems, nuclear power plants, aircraft, tanks, automobiles, refrigerators, etc. Today, within the Department of Defense, there are more than 15,000 networks and approximately 25,000 servers

[16]Department of Defense, Joint Publication (JP) 1-2, *Dictionary of Military and Associated Terms* (Washington, DC: Government Printing Office, 2012), 77, http://ra.defense.gove/documents/rtm/jp1_02.pdf (accessed 29 January 2013). RAND Corp gives credit for this definition to former DDS Gordon England (12 May 2008).The information environment (IE) is the "aggregate of individuals, organizations, and systems that collect process, disseminate, or act on information," 148. JP 3-13 defines three dimensions of the IE: physical, informational, and cognitive. The 2011 JP1-2 listed the definition of information as "1. Facts, data, or instructions in any medium or form. 2. The meaning that a human assigns to data by means of the known conventions used in their representation," 175. The definition has been removed from the 2012 version. JP 3-13 on information: Information is a strategic resource, vital to national security, and military operations depend on information and information systems for many simultaneous and integrated activities. Additionally, in the 2012 version, the definition of information operations condensed the 2011 phrase, "The integrated employment of the core capabilities of electronic warfare, computer network operations, military information support operations, military deception, and operations security," 175. To "The integrated employment, during military operations, of information-related capabilities," 148.

visible to the Internet supporting roughly 3.7 million cyber-credentialed people.[17] The reach and infiltration of cyberspace is projected to increase at an exponential rate (in some categories), such that by 2025 there may be 5.5 billion global users and 50 billion devices accessing information available on 3 billion host servers.[18]

Characteristics of Cyberspace Operations

> Cyberweapons, of course, have neither the precision of a drone nor the immediate, horrifying destructive power of the Bomb. Most of the time, cyberwar seems cool and bloodless, computers attacking computers.[19]
>
> —David Sanger, *The New York Times*

Cyberspace exists across all the other domains of warfare. The simplest explanation for this is because cyberspace is based on communication of data, information, and instructions; an inextricable element of operations in every domain. Operations on the data, information, and instructions passed in cyberspace can have digital (monitor, steal, alter, destroy), kinetic (due to automation of machine controls) and cognitive (influence) effects. In addition, operations targeting the network infrastructure can be used to disrupt, deny and degrade friendly use and transfer of information. These operations can be and are applied offensively, defensively, and in support roles in any of the domains of land, air, sea, or space. The fact that cyberspace exists

---

[17]House Armed Services Committee, *Statement by Teresa M. Takai Department Of Defense Chief Information Officer Before the House Armed Services Committee Subcommittee on Emerging Threats and Capabilities on Fiscal Year 2013 Budget Request for Information Technology and Cyber Operations Programs*, March 20, 2012, http://armedservices.house.gov/index.cfm/files/serve?File_id=d6d557bc-a941-49e0-996a-d29cf376fb0d (accessed 6 April 2013).

[18]Mark T. Maybury, "Air Force Cyber Vision 2025," Powerpoint Briefing (17 July 2012): slide 6, http://www.afa.org/events/Breakfasts/MayburyPPT.pdf (accessed 30 January 2013).

[19]David Sanger, "Mutually Assured Cyberdestruction?" *The New York Times,* June 2, 2012, http://www.nytimes.com/2012/06/03/sunday-review/mutually-assured-cyberdestruction.html?pagewanted=all (accessed 6 April 2013).

across the other domains of warfare mean all the military services are necessarily vitally interested in it. There are several characteristics of operations in cyberspace that make military action in the domain particularly attractive both to the US and to potential adversaries. These characteristics include: commercial nature of the domain, low barrier to entry, access, speed and range, ambiguity of attribution, and potential for asymmetric effects.

Commercial Nature of the Domain

The vast majority of networks and critical infrastructure in cyberspace are owned by private enterprises. A RAND Corp study points out, "the terrain of cyberspace is heterogeneous—commercial, civil, and military; domestic, foreign, multinational, and global."[20] The Internet, a significant element of cyberspace, is facilitated by infrastructure provided by private carriers known as Internet Service Providers (ISPs). In the US this includes such companies as AT&T and Verizon.[21] There are varying tiers of ISPs, but they are all private and connect homes and businesses, as well as government networks to the Internet. In addition to infrastructure providers, most government entities rely on purchase of commercial off the shelf (COTS) networking devices to operate their internal networks. This category of devices includes items such as Cisco or Netgear routers, modems, and Wi-Fi transceivers. Further, computing devices themselves including servers, desktops, laptops, and mobile devices are largely purchased from commercial vendors vice dedicated military acquisition programs. Many software programs used by the military are also commercially produced. This includes operating systems like Microsoft Windows and applications such as Adobe Acrobat. Finally, many traditionally military

---

[20]Mesic et. al., *Air Force Cyber Command (Provisional) Decision Support,* 11.

[21]Clarke and Knake, *Cyber War: The Next Threat to National Security and What to Do About It,* 74.

produced and operated services are now obtained commercially to some degree. This includes satellite communication bandwidth and imagery, as well as increased reliance on contractors to support military operations in combat zones. The large role the commercial sector plays in cyberspace has implications for military operations.

Commercial hardware and software can be the source of significant vulnerabilities. Jeffery Carr, in *Cyber Warfare*, illustrates this point with a discussion of the Chinese company Huawei, closely linked to the PRC government and suspected of participating in Chinese cyber operations. Huawei successfully merged with the US Symantec Corp and then subsequently won contracts providing hardware and software to the US government. Carr points out potential security threat examples including malicious code passed to Huawei hardware through updates or the insertion of backdoors into the hardware during production.[22] The large commercial presence in the domain also complicates strategy and targeting for the military. Dual use infrastructure and services such as Internet ISPs and lease of bandwidth from commercial communication satellites by the military raise difficult questions about whether they become valid targets because they enable military action. The significant commercial nature of cyberspace will continue to present vulnerability and policy challenges for military operators and strategists.

Low Barrier to Entry

The US has built a peerless conventional force at enormous expense that adversaries are interested in bypassing. PLA Army Colonels Liang and Xiangsui in *Unrestricted Warfare* highlight the incredible cost of US weapons systems such as the F-22 and the need to avoid the

[22]Carr, *Inside Cyber Warfare*, 214-215.

economic trap of developing similar platforms.[23] A 2011 Government Accountability Office study highlighted the fact that technical and economic barriers to entry into the cyber domain are low.[24] Commercially available and extremely affordable computer hardware, cheap and widely available access to the Internet, and the wide availability of information underpin this low barrier. Additionally, diverse and widely available forms of available human labor contribute to the low barrier to entry into cyberspace operations. In post-industrial societies where production efficiencies reduce the number of low skilled factory jobs, competitive advantage between workers lies in the exploitation of their brain power. The size of the potential labor pool within a nation or for hire abroad will limit the cost of cyber knowledge in developing economies. In the information age, knowledge work is treated as a commodity to be bought as cheaply as possible.[25] In addition to the availability and low cost of labor, some states such as Russia and China are leveraging nationalistic youth movements and hacker unions to conduct cyberspace operations. The Russian government and intelligence agencies also utilize well known ties with criminal organizations to extend cyberspace operations.[26] These policies in essence provide the governments concerned with an essentially cost free cyber work force augmentation.

One effect of the low cost of entry is a significant increase in the range of conflict and in the number of potential actors. Capitalizing on operations in cyberspace allows nations to

---

[23] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House, February 1999), 10-33, http://www.cryptome.org/cuw.htm (accessed 6 April 2013).

[24]GAO, "Defense Department Cyber Efforts: DOD Faces Challenges in its Cyber Activities," 1.

[25]Brett Glass, "Smart, Happy People Make for Good Security," *Boardwatch* 13, no. 11 (1999): 164-166, http://search.proquest.com/docview/225533273?accountid=28992 (accessed 6 April 2013).

[26]Carr, *Inside Cyber Warfare*, 90-91, 130.

partially bypass the establishment of large, heavily equipped armed forces and still have capability to initiate conflict with powerful actors like the US. State sponsored cyberspace forces are thus joined by disgruntled insiders, hack-tivists (hacker activists), non-state political organizations, criminal networks, corporations, and terrorists. Jeffrey Carr detailed cyber operations efforts currently active in 25 countries and noted his list was incomplete due to publishing deadlines.[27] The low barrier to entry suggests the standup of at least some cyberspace operational capability is likely to be pursued by the majority of world nations.

The low barrier to entry in cyberspace does not, however, guarantee a country will develop effective military operations in cyberspace. Effective military application in cyberspace goes well beyond the capabilities of individual hackers. Gregory Rattray asserts that highly complex organizations are required to effectively develop cyber attacks that can gain a desired level of political influence. He compares the large number of targeteers, engineers, and system analysts as well as crews needed for the strategic bombing campaign in World War II to what would be needed for strategic cyber attack.[28]

Access

There are four elements that make access an important characteristic of cyberspace operations. The first element is the virtual elimination of borders. Internet development was based on an open architecture that would allow entities to develop their own network, then, through a

---

[27]Ibid, 243.

[28]Gregory Rattray, *Strategic Warfare in Cyberspace* (Cambridge, MA: Massachusetts Institute of Technology, 2001), 192, http://books.google.com/books?hl=en&lr=&id lVbQ4AxfYaMC&oi =fnd&pg=PP1&dq=Strategic+Warfare+in+Cyberspace&ots= OGA8sGQLiC&sig=Z-QOrM5FTcHxWbkLKE-LkiPTAzk#v=onepage&q=Strategic% 20Warfare%20in%20 Cyberspace&f=false (accessed 12 September, 2012).

standard protocol connect it to other networks, the result being a globally connected network of networks.[29] The interconnectedness of the Internet means traditional political borders of states have little meaning and actors can reach anywhere a connection to the Internet exists.[30] In addition, individual networks usually have multiple outward facing connection points to the Internet allowing multiple access points to targets within the network. Further, the interconnectedness reduces that defensive strength of a system to the weakest (computer) link in the net. Access is potentially only limited by the "connectedness" of a target to cyberspace. Two broad examples of targets with limited access via cyberspace include developing countries that have very little information infrastructure and organizations that isolate their local network from the internet. The first case is an example of the man-made nature of cyberspace and the second is a self-imposed limitation in the name of defense.

The second element of access is the inherent vulnerabilities of software programs. Gregory Rattray warned in 1999, "in today's environment, governments and military organizations have little control over the development or diffusion of information technologies."[31] Adoption of commercial software programs by military organizations opens access ports for adversaries to conduct operations within their networks. Programs such as Microsoft Windows contain tens of millions of lines of code. As Richard Clarke highlights in

---

[29]Cerf, et al., "Brief History of the Internet," 3-4.

[30]This characteristic can be extended to networks that are not connected to the Internet, but that have access terminals that can be hacked such as "closed" radio and satellite networks. In Hiltz and Turoff's *The Network Nation* (1978) which was written at a time when only a few government and academic agencies had the ability to participate in what was then called computer mediated communication, the authors envisioned an interconnected world, "who's boundaries are demarcated only by the political decision of those governments that choose not to become part of an international computer network."

[31]Rattray, *Strategic Warfare in Cyberspace*, 227.

Cyber War, a number of exploitable mechanisms can be accidentally or intentionally inserted into the code which current production methods fail to detect before release. Once the software is released, cyber operators hunt out code errors and back doors in the software for exploitation. Unintentional exploitable errors in software have become known as "zero day" vulnerabilities. Exploitation of zero day errors is so lucrative it has spawned an industry to uncover and auction such errors to the highest bidder.[32] The issue is not limited to end user computer operating systems and applications software. The devices that make up the infrastructure of networks are also accessible. In late 2012 an attack on DSL modem firmware was discovered in Brazil which redirected user internet page requests to exploitive Domain Name Servers that effectively allowed criminals to pilfer banking credentials. It was estimated that millions of internet users were affected in the country. While users failing to update firmware were a significant cause of the access, the report indicated that the manufacture design of a widely used chipset was also a factor in the attack.[33] The example indicates that actors will seek and exploit errors in software and firmware across the spectrum of devices operating in, or used to operate, networks in cyberspace.

The third element of access in cyberspace is vulnerability of the hardware production chain. The globalization of computer and network hardware manufacturing has vastly expanded the number of producers, which limits national control of the production chain. The globalization allows actors the opportunity to insert malicious hardware and software at the point of production. This form of access is the cyberspace analogue of the cold war sleeper agent.

---

[32]Tech2 News Staff, "WatchGuard lists its security predictions for 2013," *tech2*, December 11, 2012, http://tech2.in.com/news/general/watchguard-lists-its-security-predictions-for-2013/634642 (accessed 3 January 2013).

[33] Fabio Assolini, "The Tale of One Thousand and One DSL Modems," *Securelist*, October 1, 2012, https://www.securelist.com/en/blog/208193852/The_tale_of_one_thousand_and_one_DSL_modems (accessed 6 April 2013).

The fourth element of access is exploitation of human psychology. Human curiosity was exploited to great effect in 2008 when an individual picked up a thumb drive from a CENTCOM parking lot and inserted it into a government system, allowing malware to transfer data from both classified and unclassified systems to foreign servers. Along with the damage from loss of data, the DoD was forced to enact constraining policies such as prohibiting the use of USB memory drives.[34] Human socialization is also exploited to gain access. Spear phishing techniques entice users to open files or connect to websites that contain malicious code. This technique involves some sort of deception that lures the victim into "trusting" the exploit and enticing them to bypass organizational defense policies either intentionally or unintentionally.[35]

The great emphasis DoD is placing on countering nation states' anti-access, area denial initiatives in the air, land, and sea domains indirectly highlights the attractiveness of the open access environment that currently exists in cyberspace. Access issues are likely to change significantly in the future as the current state of affairs is recognized as a significant vulnerability. Countries that have the ability are actively limiting the openness of networks. The Chinese have been working since 2001 to make outside access to their networks significantly more difficult.[36] Iran, target of the Stuxnet Virus, has publicly declared it will attempt to replace the Internet with a domestic Intranet system.[37] The US military is also seeking to reduce access vulnerabilities

---

[34]William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* 89, no. 5 (September/October 2010): 97, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA527707&Location=U2&doc=GetTRDoc.pdf. (accessed 24 April, 2013).

[35]Norton by Symantec, "Spear Phishing: Scam, Not Sport," Norton by Symantec, http://us.norton.com/spear-phishing-scam-not-sport/article (accessed 6 April 2013).

[36]Bill Gertz, "China Blocks U.S. From Cyber Warfare," *Washington Times*, May 12, 2009, http://www.washingtontimes.com/news/2009/may/12/china-bolsters-for-cyber-arms-race-with-us/ (accessed 6 April 2013).

[37]Eleanor Keymer, "Iran to Take Key Ministries Offline to Avoid Cyber Attacks," *Jane's*

through initiatives such as the *DoD IT Enterprise Strategy and Roadmap*. One such initiative will reduce the number of connection points between DoD networks and the Internet, thereby reducing the size of the attack surface.[38] As an example, the Air Force implemented network architectural changes that reduced the number of Internet access points from 140 to 16.[39] Organizations will have to make difficult tradeoffs between the collaborative power enabled by open access networks and restrictive policies required to prevent exploitation, theft or destruction of their data and systems that process it.

Speed and Range

Speed and range characteristics make operations in cyberspace particularly attractive. Speed in cyberspace is bounded by the length of time it takes information to travel across the network it flows on. Since electromagnetic waves travel at near the speed of light and electrical signals in wires travel at 40 percent the speed of light (at the low end), the time (in an ideal case) for a signal to traverse the circumference of the earth is under a second.[40] Thus the time lapse

---

Defence Weekly, August 9, 2012, https://janes.ihs.com.lumen.cgsccarl.com/CustomPages/Janes/DisplayPage.aspx?DocType=News&ItemId=+++1516425&Pubabbrev=JDW (accessed 6 April 2013). The article also noted that cyber-security experts are skeptical whether this initiative is realistic.

[38]U.S. Department of Defense, *Department of Defense Information Technology Enterprise Strategy and Roadmap Version 1.0* (September 6, 2011): 6. http://dodcio.defense.gov/Portals/0/Documents/Announcement/Signed_ITESR_6SEP11.pdf (accessed 22 April 2013).

[39]Suzanne M. Vautrinot, "Sharing the Cyber Journey," *Strategic Studies Quarterly* 6, no. 3 (Fall 2012): 85, http://www.au.af.mil/au/ssq/2012/fall/fall12.pdf (accessed 7 April 2013).

[40]Calculated using the following: straight line wire or line of sight satellite with no switching delays. Circumference of earth = $4x10^7$m, geostationary orbit = $3.5x10^7$m, speed of light = $3x10^8$m/s. The time for a signal to reach a satellite in geostationary orbit and back is approximately .233 seconds. Signal for a fiber/wire strung around the globe could complete a trip in .13 to .23 seconds.

from initiation of an attack until it reaches the target is mentally negligible. Lieutenant Colonel David Hollis emphasized this point in a 2010 article:

> [cyber attacks] occur near the speed of light and in real time, and often can impact the entire spectrum of the cyberspace domain simultaneously without notice or intelligence indicators. This instantaneous nature and the ability to attack the entire domain simultaneously are characteristics that potentially make the cyberspace domain a much more dangerous and vulnerable domain.[41]

The significant advantages of speed and range in cyberspace were also noted by Secretary of Defense Leon Panetta in 2012 warnings about adversary exploitation of DoD Global Information Grid vulnerabilities to degrade US military operations.[42]

Two important points must be made about speed. First, the ability for malicious code to travel across cyberspace at the speed of light does not mean that malicious routines can be produced at the speed of light. The widely publicized Stuxnet virus, which *New York Times* journalist David Sanger revealed last year as a US produced cyber weapon, was so complicated it may have taken four years to write the code.[43] Commentators often lament the seeming ease with which US cyber systems can be exploited or taken down.[44] Both Gregory Rattray and Paul Rosenzweig suggest the skills necessary to develop and launch complex offensive cyber weapons

---

[41]Hollis, "USCYBERCOM: The Need for a Combatant Command Versus a Subunified Command," 50.

[42]Suzanne El Sanadi, "Potecting the Grid: DOD Fortifies Itself Against Threat of Cyber Attacks," Heritage Foundation Blog, entry posted 14 June 2012, http://blog.heritage.org/2012/06/14/protecting-the-grid-dod-fortifies-itself-against-threat-of-cyber-attacks/ (accessed 14 January 2013).

[43]Paul Rosenzweig, "The Stuxnet Story and Some Interesting Questions," LAWFARE blog, entry posted 2 June 2012, http://www.lawfareblog.com/2012/06/the-stuxnet-story-and-some-interesting-questions/ (accessed 8 February 2013). Israel is also implicated in the production of STUXNET.

[44]For example, GAO report 11-421 to Congress on Cyber personnel issues asserted "a handful of programmers could cripple an entire information system," 1.

currently only resides in highly sophisticated organizations such as US, Russian, and Chinese cyber warfare units.[45] If true at the moment, it may not be so forever. Journalist Robert McGarvey points out that the malware industry is going through business-like price reduction cycles. He alludes to the fact that botnets may now be available for rent by the hour at costs as low as several hundred dollars a day.[46] Business innovation, even for nefarious purposes, will likely result in attack methodologies being packaged and marketed to organizations and governments interested in operating in cyberspace. In addition, it is probable that organizations will seek methods to automate code writing to either originate or modify attacks in order to seek advantage in an environment where maneuver occurs on the scale of microseconds.[47]

---

[45]Ryan Naraine, "10 security stories that shaped 2012, Guest Editorial by Costin Raiu," *ZDNet.com*, December 10, 2012, under "Topic:Security" http://www.zdnet.com/10-security-stories-that-shaped-2012_p2-7000008576/ (accessed 3 January 2013). Another example is the recently discovered Flame malware. "Flame is arguably one of the most sophisticated pieces of malware ever created. When fully deployed onto a system, it has more than 20 MB of modules which perform a wide array of functions such as audio interception, bluetooth device scanning, document theft and the making of screenshots from the infected machine. The most impressive part was the use of a fake Microsoft certificate to perform a man-in-the-middle attack against Windows Updates, which allowed it to infect fully patched Windows 7 PCs at the blink of an eye. The complexity of this operation left no doubt that this was backed by a nation-state."

[46]Robert McGarvey, "2013's 5 Biggest Online/Mobile Cyber Threats," *Credit Union Times.com*, December 10, 2012, http://www.cutimes.com/2012/12/10/2013s-5-biggest-online-mobile-cyber-threats?ref=hp&t=technology&page=4 (accessed 3 January 2013).

[47]As a business example of this, during the first week of February, CNBC reported an investigation into suspicious futures trading activity related to natural gas. With the benefit of high speed trading technology, it appears an entity executed trades valued at $4.6 million dollars 400 milliseconds before the release of a government report containing information on gas storage levels that made the trades profitable. Eamon Javers, "Unusual Natural Gas Trade Raises Questions," *CNBC.com*, January 31, 2013, http://www.cnbc.com/id/100425191 (accessed 6 April 2013). Also see Lt Col William B. Osborne, et. al.'s "Information Operations: A new War-Fighting Capability" (research paper presented to Air Force 2025, August 1996), http://csat.au.af.mil/2025/volume3/vol3ch02.pdf, for very futuristic treatment of command decision making problems in an environment of massive available information delivered at the speed of light.

Difficulty of Attribution

Programmers have devised a variety of techniques which capitalize on the open architecture and routing protocols of the Internet to either mask or obfuscate their activities. This means attribution for cyber-attacks can be difficult if not impossible. Jeffrey Carr in his Open Source based examination of cyber warfare outlines several examples of attribution difficulties in Cyberspace. In depth investigation into the origin of 2009 attacks against US and South Korean government websites illustrates the issue. The South Koreans originally placed blame on North Korea for the botnet-facilitated attacks. The suspected control server running the botnet, however, was traced to a private company in London, UK. Further work revealed the actual control server was located in Miami, Florida and used Virtual Private Network (VPN) routines to implicate the London server. The location of the malicious servers in the US and UK implicated allies of South Korea, but did not identify the actual perpetrator of the attack. In addition, it was determined that the botnet that executed the attacks consisted of more than 150 thousand computers located in 74 countries, making multiple nations unsuspecting accomplices.[48] The current inability to clearly attribute cyber-attacks greatly complicates the job of political and military leaders to seek redress or to retaliate. Governments will seek measures to minimize or eliminate this particular characteristic of cyberspace in the future. For example, the Defense Advanced Research Projects Agency (DARPA) has initiated Plan X, which amongst other things is an effort to map the entire Internet.[49] Such a map could help forensic investigators track down the origin of attacks. Also,

---

[48]Carr, *Inside Cyber Warfare,* 77-79. Carr also uses the cyber attacks on the nation of Georgia to illustrate the point. A case in which the control server was also located in the US, belonging to a company controlled by Russian organized crime.

[49]Richard Steinnon, "Operation Olympic Games, Project X, and the Assalut on the IT Security Industry," *Forbes.com,* June 4, 2012, http://www.forbes.com/sites/richardstiennon/2012/06/04/operation-olympic-game-project-x-and-

international conventions such as the Budapest Convention on Cybercrime incorporate cooperative investigation clauses between states.[50] Failure to sign on to such agreements may better indicate a nation's hostile cyber intent in a particular incident and could possibly be used as attribution criteria when an attacked state considers diplomatic or military response to a cyberattack.

Potential for Asymmetric Effects

The characteristics of cyberspace operations discussed so far are the reason cyberspace has the potential for asymmetric effects. Asymmetry itself is also what makes it such an appealing operating environment. As General Alexander puts it, "Cyber represents an alternative; it can provide kinetic effects while using non-kinetic capabilities." [51] US dominance in other domains of warfare also makes cyber operations attractive to potential adversaries. Strategists from near peers China and Russia carefully studied the 1991 and 2003 US victories over Iraq. The strategists drew two major conclusions, the US conventional capability would be difficult to match and that great potential lies in "informationized" warfare.[52] Unable to match the conventional might, states have placed emphasis on developing cyberspace capabilities. The appeal of cyberspace may be reinforced by self-declared US vulnerabilities and the large volume

---

the-assault-on-the-it-security-industry/ (accessed 22 April 2013).

[50] See Appendix C for further discussion of the Budapest Convention on Cybercrime.

[51]Vautrinot, "Sharing the Cyber Journey," 81.

[52]Dean Cheng, "Chinese Lessons From the Gulf Wars," in *Chinese Lessons from Other Peoples' Wars*, edited by Andrew Scobell, David Lai and Roy Kamphausen (Carlyle Barracks: Strategic Studies Institute, U.S. Army War College, November 2011), 153-165, http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=1090 (accessed 22 April 2013); and Thomas, *Recasting the Red Star: Russia Forges Tradition and Technology through Toughness*, 169-170.

of press covering this topic.[53] Smaller states that may feel pushed around by the US are also interested in cyberspace. Jan Kallberg offers the example of US Space assets used to monitor the actions of authoritarian regimes. Such regimes will find the opportunity to directly or indirectly destroy US space assets through cyberspace attacks attractive due to limited risk of attribution and traceability.[54] The potential for asymmetric effects in cyberspace will both increase the number of actors operating in the domain and affect the strategic calculations of those actors, from individuals to states.

Finally, synergy provided by taking advantage of multiple characteristics of the cyberspace environment will add motivation for actors to operate in cyberspace. For example, when the speed and range of cyberspace are combined with access, an attacker can utilize persistent presence to devise a way to penetrate defenses and then maneuver against them once into a target. A recent warning from the banking industry illustrates the point: "some cyber-criminals are learning from the tactics used by a credit union to detect and thwart them – and they are coming back in 90 to 120 days with an improved scheme to loot the institution and its members' accounts."[55] The characteristics of cyberspace operations explored above illuminate why cyberspace operations hold such appeal and are a contributing factor to the current state of the cyberspace operational environment.

---

[53]Rattray, *Strategic Warfare in Cyberspace*, 469-488.

[54]Jan Kallberg, "Designer Satellite Collisions from Covert Cyber War," *Strategic Studies Quarterly* 6, no. 4 (Spring 2012): 124-136, http://www.dtic.mil/dtic/tr/fulltext/u2/a562109.pdf (accessed 6 January 2013).

[55]McGarvey, "2013's 5 Biggest Online/Mobile Cyber Threats."

CYBERSPACE OPERATIONAL ENVIRONMENT

This section focuses attention on the current cyberspace operational environment and issues that frame the primary discussion of if, when, and how a separate Cyber Force might be necessary or feasible. First, the contested nature of the cyberspace domain is examined which shows the domain is very active with military, espionage, and criminal actors. Then, US Chinese and Russian thinking on cyberspace operations are examined.

A Contested Domain

Cyberspace is a contested domain. A diverse set of actors are engaged in espionage, covert action, harassment, and criminal activities to achieve political and economic objectives. Current articles on *cybersecurity* list several categories of actors/threats in cyberspace including, nation states, transnational criminal and terrorist organizations, large corporations, insiders, and hacker groups. [56] Actors are conducting operations against other actors in their category and also across categories. States are targeting corporations as well as other states. Criminal organizations are targeting corporations, individuals and some state run entities. Hackers are targeting corporations and states. The operating environment is complex. Adding to the complexity is the fact the international community has not clearly defined what constitutes an act of war in cyberspace. General Keith Alexander in Senate testimony outlined that cyberspace attacks should be evaluated in terms of the laws of armed conflict and that cyber effects which disrupt or destroy critical national infrastructure may cross the line and constitute an act of war.[57] The lack of

---

[56]Naraine, "10 security stories that shaped 2012, Guest Editorial by Costin Raiu," 2.

[57]Senate Armed Services Committee, "Hearing To Receive Testimony On U.S. Strategic Command And U.S. Cyber Command In Review Of The Defense Authorization Request For Fiscal Year 2014 And The Future Years Defense Program," 8, http://www.armed-

clarity on what constitutes an act of war is important in general because it increases the chance of international misunderstandings and may contribute to military escalation that may otherwise be avoided or mitigated.[58]

The DNI outlined two forms of cyberspace threats in the 2013 Worldwide Threat Assessment brief to Congress; cyberspace attacks and cyberspace espionage. Jeffrey Carr estimates that over 120 countries are developing cyberspace operations capabilities. [59] Revelation of the US as originator of the Stuxnet worm, which destroyed Iranian nuclear centrifuges, gave the US the distinction of being one of the few acknowledged nations to conduct a cyberspace attack with kinetic effects. Iran joined this group in 2012 with the Shamoon virus that destroyed data on an estimated 30,000 computers belonging to Saudi Aramco.[60] Iran is also suspected of conducting disruptive attacks on US banks on Wall Street over the last summer, where at least 140 denial of service attacks have occurred.[61] Evidence of Chinese cyberspace attack capabilities were accidentally and visibly revealed in a Chinese military television program which showed screen shots of an attack software program.[62] Russian hacktivists believed to be supported by the

---

services.senate.gov/Transcripts/2013/03%20March/13-09%20-%203-12-13.pdf (accessed 6 April 2013).

[58]See Appendix C for discussion of international efforts to address this issue.

[59]Carr, *Inside Cyber Warfare,* 161.

[60]Naraine, "10 security stories that shaped 2012, Guest Editorial by Costin Raiu," 2.

[61]Senate Armed Services Committee, "Oversight: U.S. Strategic Command and U.S. Cyber Command," Webcast video of hearings (March 12, 2013), http://www.armed-services.senate.gov/hearings/event.cfm?eventid=0daf354e2970a9db3a6d0023abe58a27 (accessed 16 March 2013).

[62]Matthew Robertson and Helena Zhu, "Slip-Up in Chinese Military TV Show Reveals More Than Intended," *Epoch Times,* August 21, 2011, http://www.theepochtimes.com /n2/china-news/slip-up-in-chinese-military-tv-show-reveals-more-than-intended-60619.html> (accessed 9 December 2012).

Russian Government disrupted banking services during the 2008 war with Georgia. A Georgian NATO representative indicated the attacks fomented bank runs threatening the fabric of Georgian economic stability.[63] The ability to destroy physical assets via their associated computer control systems continues to evolve. McAfee Corporation reported that researchers were able to locate several critical infrastructure control devices simply by searching for them on Google. [64] Widespread power outages that degrade or threaten lives by knocking civilization back to pre-electrified days for an extended period or rail/aircraft accidents caused by manipulating transportation control systems cause the greatest concern.[65] Researchers recently demonstrated the ability to induce wirelessly a high voltage shock to a pacemaker. The potential to kill enemy combatants via human-machine interfaces is now science fact, not science fiction.[66] US Army COL Jayson Spade, in a 2012 Monograph on Chinese cyber threats warned:

> America must recognize that its superpower status is challenged by the People's Republic of China's cyber power. The United States must use China's computer network exploitation capabilities as a minimum standard for developing integrated cyber policy, security and defense.[67]

While the US military may lack peers in the conventional war fighting arena, such advantages in cyberspace are neither so clearly evident nor guaranteed in the future.

---

[63]Author Interview w/ Georgian NATO representative, October 2012.

[64]McAfee Corporation, *Smarter Protection for the Smart* Grid (Santa Clara: McAfee, 2012), 7, http://www.mcafee.com/us/resources/reports/rp-smarter-protection-smart-grid.pdf (accessed 6 April 2013).

[65]The 2013 US Worldwide Threat Assessment deems such attacks unlikely at present due to the sophistication of cyber program required restricted to nations at this point.

[66]Tech2 News Staff, "WatchGuard lists its security predictions for 2013," Internet Article, December 11, 2012. http://tech2.in.com/news/general/watchguard-lists-its-security-predictions-for-2013/634642 (accessed 3 January, 2013).

[67]Jayson C. Spade, *China's Cyber Power and America's National Security* (strategy research project, Army War College, 2011), 50.

National espionage exploits in cyberspace have been widely publicized. The Flame and Gauss malware programs, which are thought to be targeted against Iran are highly sophisticated pieces of software and included the capability to take screen shots and turn on computer recording devices.[68] A rising volume of exploits against DoD networks merits attention. Over a 22 month period, Army Cyber Command blocked 400,000 unauthorized access attempts, 4,000 known malicious websites, and 400 email phishing campaigns. [69] Statistics from the other services tell a similar tale. The defense industrial base has also been the target of espionage for decades. Recently, large amounts of data were stolen from Joint Strike Fighter subcontractors and secure teleconferences discussing program technologies were hacked into.[70] Cyber actors are also attempting to gain advantage by stealing corporate intellectual property. Eric Gross, a senior security engineer for Google warned that corporations are being targeted by nation states, both friendly and unfriendly.[71] In addition, US intelligence analysts have implied the Chinese government encourages hackers to conduct theft of intellectual property from corporations.[72] A

---

[68]Eleanor Keymer, "Iran to Take Key Ministries Offline to Avoid Cyber Attacks."

[69]House Armed Services Committee, *Statement by Lieutenant General Rhett Hernandez Commanding General U.S. Army Cyber Command/2nd Army Before the Emerging Threats and Capabilities of the House Armed Services Committee*, July 25, 2012, http://armedservices.house.gov/index.cfm/hearings-display?ContentRecord_id=c0de6683-61a9-4b83-b443-8a8c45ff5009&Statement_id=7fc85bab-d453-4e30-947e-03bb1a48f5c9&ContentType_id=14f995b9-dfa5-407a-9d35-56cc7152a7ed&Group_id=41030bc2-0d05-4138-841f-90b0fbaa0f88&MonthDisplay=7&YearDisplay=2012 (accessed 12 September 2012).

[70]John Reed, "Did Chinese Espionage Lead to F-35 Delays?" *DefenseTech*, February 6, 2012, http://defensetech.org/2012/02/06/did-chinese-espionage-lead-to-f-35-delays/ (accessed 6 April 2013).

[71]Eric Gross, "Some tech-talks in Security, Cryptography, and Privacy," 2010 Google Faculty Summit: Security at Scale, video presentation, http://research.google.com/pubs/SecurityCryptography andPrivacy.html (accessed 14 January 2013).

[72]Ken Dilanian, "US Spy Agencies to Detail Cyber-Attacks from Abroad," *Los Angeles Times*, December 6, 2012, http://www.latimes.com/news/nationworld/nation/la-na-cyber-intel-

recent report by Mandiant Corporation linked a threat they designated as Advanced Persistent Threat 1 (APT1) to the People's Liberation Army. Mandiant reported APT1 has been active since 2006, stolen hundreds of terabytes of data from 141 organizations, and conducted 1,905 intrusions.[73] Espionage is an age old inter-state practice. The ability to penetrate outside networks while attempting to protect internal networks will remain an ongoing challenge for nations operating in cyberspace.

Criminal activity in cyberspace, while primarily a law enforcement issue, has relevance to military organizations. The participation of DoD enablers in the War on Drugs is an example of why this is true. The interconnection of DoD cyber forces with law enforcement agencies like the FBI, indicate the high likelihood of a similar enabling role in defeating cyberspace crimes. Criminal activity is rampant in cyberspace. According to Symantec Corporation malicious software production is on the rise, with 1.5 million new pieces fielded in just the first quarter of 2012, one resultant being an estimated 72 percent of Americans have been hacked. No platform or operating system seems to be able to stay immune. In 2012, Apple's operating system, widely thought to be secure, was penetrated by malware known as Flashback.[74] A technique known as Man-in-the-Browser, which targets web browsers, has been used to steal account information of individuals from "the cloud."[75] Mobile devices are a growth area for cybercrime. More than 35,000 malicious Android programs were discovered in 2012.[76] Malware growths rates have

---

20121207,0,1598259.story (accessed 9 December 2012).

[73]Mandiant "Intelligence Center Report," http://intelreport.mandiant.com/ (accessed 18 March 2013).

[74]Naraine, "10 security stories that shaped 2012, Guest Editorial by Costin Raiu."

[75]Tech2 News Staff, "WatchGuard lists its security predictions for 2013."

[76]Naraine, "10 security stories that shaped 2012, Guest Editorial by Costin Raiu."

topped 500 percent over some recent periods.[77] Malware known as Eurograbber facilitated theft of 36 million Euros from 30,000 accounts by exploiting cell phone SMS authentication tools. Large volumes of customer information have been stolen from corporations such as Sony and Citi.[78] Storage of large volumes of data "in the cloud" has resulted in corresponding massive losses when systems are penetrated. In addition, cyber criminals have exploited previously mentioned critical infrastructure weakness by extorting utility providers. A McAfee study reported that one in four power companies globally have been extorted for an estimated hundreds of millions of dollars.[79] Cybercrime may directly affect DoD in the future. The Defense Information Services Agency's (DISA) strategy to move to mobile and cloud computing paradigms will require robust defenses to prevent data exploitations similar to that suffered by corporate America. The contested nature of cyberspace is a great threat to global stability. An environment such as described above requires norms and legal structures to counter destabilizing forces.[80] Understanding that cyberspace is a contested environment, examination now turns to military thinking on war and operations in cyberspace.

Strategic Cyber War and Cyberspace Operations Thinking

Sun Tzu adages appear to be influencing current thoughts on cyberspace strategy. He opens his oft cited and revered text with an admonition: "Warfare is the greatest affair of the state, the basis of life and death, the Way to survival or extinction. It must be thoroughly

---

[77]Claudette Roulo, "Cybercom Chief: Culture, Commerce Changing Through Technology," *American Forces Press Service*, October 12, 2012, http://www.defense.gov/news/newsarticle.aspx?id=118201 (accessed 30 December 2012).

[78]Ibid.

[79]McAfee, *Smarter Protection for the Smart Grid*, 5.

[80] See Appendix D

pondered and analyzed."[81] While this may be true in many ways, it sets the stage for the rest of his work to cast Platonic shadows into the cave military strategists inhabit. One such shadow of particular interest to cyberspace strategists is his declaration, "[s]ubjugating the enemy's army without fighting is the true pinnacle of excellence."[82] This declaration entices the strategist to believe, if he is just smart enough to figure it out, that there is a way to defeat your enemy without enduring the bloody clashing of armies. The advent of aircraft lured early airpower strategists to believe that bombing enemy populations or industrial production centers, could break the will of the people or leadership and force an enemy to capitulate before millions died on the battlefield. But events in WWII showed that civilian casualties strengthened resolve, mass production facilities could be put underground or dispersed, and the war appetite of ambitious leaders was not curbed. The goal of imposing political will, when the struggle has devolved to military means, without bloody retribution by the adversary remains elusive. The domain of cyberspace has offered strategists a new realm to once again consider this grand dream. This section reviews US, Chinese, and Russian thinking on Strategic Cyber War.

Strategists have been considering war and warfare in cyberspace since at least the close of the 1991 Gulf War between the US led coalition and Iraq. Military strategists in Russia and China examined the resounding and rapid victory over Iraq's feared army in search of lessons to be applied to their own situations.[83] The strengths and weaknesses of cyberspace were a major area of focus. In the intervening years thought by a variety of actors has been put into what is now called cyberspace and cyber operations, but has also been called Information Warfare, Network

---

[81]Sun-Tzu, *The Art of War*, trans. Ralph Sawyer (Boulder: Basic Books, 1994), 177.

[82]Ibid, 177.

[83]Carr, *Inside Cyber Warfare*, 166-177.

Warfare, Net-centric Warfare, etc. Thinking in Russia and China appears to be partly based on both reaction to US actions and published US cyberspace doctrine. Within the US, strategic emphasis in cyber war discussions is typically placed on defense.

Chinese strategists are aware of the current inability of PLA forces to match US large-scale conventional warfare capabilities. Additionally, there is an expressed view that conflicts between the great powers will likely be conducted as limited wars. The proposed cyber strategy in these limited wars will be to impose costs on the adversary that are so great capitulation occurs before conventional fighting breaks out. Cyberspace becomes a preferred domain of action for this strategy due to the assessment that those who are most reliant on cyberspace are most vulnerable. John Farrell and Adam Lowther suggested this would be just the aim of the PRC in a Taiwan or South China Sea Scenario.[84] All interests of a nation connected to cyberspace, not just the military, could and should be targeted in order to coerce capitulation. This viewpoint was espoused by PLA Colonels Liang and Xiangsu in *Unrestricted Warfare* (1999) with passages such as, "there is no longer any distinction between what is or is not the battlefield. Spaces in nature including the ground, the seas, the air, and outer space are battlefields, but social spaces such as the military, politics, economics, culture, and the psyche are also battlefields."[85] Jeffrey Carr notes that China may also find cyberspace operations attractive because national leaders view war in cyberspace as a People's War. Carr suggests this viewpoint may have come about somewhat passively after the PLA took notice of Chinese civilian hacker attacks on the US following the Chinese fighter aircraft – US P-3 aircraft collision and the US bombing of the

---

[84]John F. Farrell and Adam B. Lowther. "From the Air: Rediscovering Our Raison D'etre," *Air & Space Power Journal* 26, no. 4 (July-August 2012): 74, http://www.airpower.au.af.mil/digital/pdf/issues/2012/ASPJ-Jul-Aug-2012.pdf (accessed 22 April 2013).

[85]Liang and Xiangsui, *Unrestricted Warfare*, 223-240.

Chinese embassy in Serbia.[86] Chinese thinkers since then have come to view their populace of hackers and civilian computer experts as part of their overall cyber forces, to be mobilized in time of conflict. Demographic trends add concern to this line of thinking. US Air Force Chief Scientist Dr. Mark Maybury projects China will produce 8,500 computing PhDs to the US's 3,800 by 2025.[87] Recent trends indicate that China is actively pursuing this People's War strategy through organizations such as the Honkers Union, an identified Chinese hacking organization, and by elements revealed in the Mandiant Report discussed elsewhere in this paper.[88] Chinese writing on strategic cyber war suggest "the most dangerous" scenario in a US-China conflict would include pre-emptive cyber attacks on military and DHS identified critical infrastructure targets. A combination of kinetic and non-kinetic means would be used to target communication, multi-spectral imaging, and navigation satellites, destroy or manipulate data in financial markets, induce widespread power outages in the US, and wreak havoc with transportation control systems such as the air traffic system run by the Federal Aviation Administration (FAA).

Russian strategic cyber war thinking runs along similar lines to the Chinese, but varies in implementation. Russian strategists recognize the disruptive potential of cyber attacks on adversaries' information systems as well as the increased vulnerability of those most dependent on them. A senior military advisor to President Putin in 2008 expressed in a public speech the notions that future war will emphasize attacks on command and control systems, navigation and communications, and as well as other information systems.[89] Russian Information War thinking

---

[86]Carr, *Inside Cyber Warfare*, 172.

[87]Maybury, "Air Force Cyber Vision 2025."

[88]Matthew Crosston, "Virtual Patriots and a New American Cyber Strategy: Changing the Zero-Sum Game," *Strategic Studies Quarterly* 6, no. 4 (Winter 2012): 100-117.

[89]Carr, *Inside Cyber Warfare*, 165; and Timothy Thomas, *Recasting the Red Star: Russia*

also includes a significant role for information operations (influence, psychological) on adversary political/military leadership, troops, and the general population.[90] Timothy Thomas provides a good sampling of Russian strategic cyber war thinking in *Recasting the Red Star*. Themes in Russian writings emphasize concepts related to the US idea of information dominance, including seizing the initiative in the information sphere, securing access to reliable information while denying the enemy to do the same, targeting all elements of a society's information infrastructure, and destroying enablers such as communications and navigation systems.[91] Outside of the US (and possibly Israel), Russia may have made the largest publicly exposed use of cyber operations in warfare with their operations in Chechnya, Estonia, and Georgia. These operations illuminate how Russia goes about implementing strategic cyber war ideas. Cyber attacks in the countries/territories mentioned were largely attributed to non-governmental hackers, although both Carr and Thomas make more than minor connections between the Russian government and the supposed perpetrators. The analyses suggest the Russian government is executing a strategy of indirect action to avoid direct attribution. This strategy shifts investigative focus on cyber attacks from the politico-military realm to the cybercrime realm. Russian attempts to push cyber arms control treaties in international venues, while rejecting any international law enforcement cooperation efforts are seen as the political backstop for their cyber strategy.[92] Russian cyber war efforts have thus garnered the character of being "criminalized" in the literature.

Forges Tradition and Technology through Toughness, 150.

[90]Carr, *Inside Cyber Warfare*, 167.

[91]Thomas, *Recasting the Red Star: Russia Forges Tradition and Technology through Toughness*, 149-190.

[92]Carr, *Inside Cyber Warfare*, 168.

A survey of writing on US strategic thinking on cyberspace reveals a trend towards focus on defense.[93] Part of the problem in defining a US military cyber strategy is the military does not have responsibility for a major portion of US cyberspace. Efforts to improving cyberspace defense include reducing the attack surface by moving from an ad-hoc, off the shelf, collection of 15,000 networks to purposely architected, interoperable, network(s) with a known set of external interfaces to the Internet.[94] Within this new network structure, DoD must be able to have situational awareness of what is going on in all parts of it. Part of building this network structure will also include creating a trusted supply chain of hardware and software vendors to further reduce the attack surface represented by "trap doors" and "zero-day defects."[95] Until that work is done (and even after) DoD will conduct emergency drills simulating an enemy that has gotten in or taken down parts of the network, so as to build and have on-hand viable work-a-rounds, otherwise known as resiliency. In addition, the mindset about information is changing. Protecting all information is being downplayed and focus has shifted to mission assurance, which requires identifying and protecting critical nodes.[96] These efforts will be prioritized because DoD networks are currently being penetrated. To further enhance cyberspace defense, all information traffic coming in is monitored to detect attacks while also internally probing networks to try and

[93] See Apprendix B for a review of US cyberspace strategy documents.

[94]Cheryl Pellerin, "Cybersecurity Involves Federal, Industry Partners, Allies," *American Forces Press Service*, November 8, 2012, http://www.defense.gov/news/newsarticle.aspx?id=118479 (accessed 30 Dec 12).

[95]James P. Farwell, "Industry's Vital Role in National Cyber Security," *Strategic Studies Quarterly* 6, no. 4 (Winter 2012): 10-35.

[96]Vautrinot, "Sharing the Cyber Journey," 83.

find vulnerabilities.[97] For the future, DoD will work to develop the ability to recognize attacks before they get into the network and to defeat them outside the network perimeter.

The offensive portion of cyberspace strategy is much less discussed in the literature. This likely is for one or both of two reasons. The first plausible reason is that the US has a well-developed offensive cyber capability that leaders are confident in, but is highly classified, so it does not receive much unclassified attention. The second reason may be focus on tactical application of cyberspace operations as enabler to action in the other domains. Regardless which is the case, it is important for future strategists to examine all aspects of war in cyberspace including the concept of strategic cyber war. Some author comments in recent articles show promise that this will be the case. In discussing the future of US Air Force Cyber operations, authors of an "Air Force 2025" study envisioned future cyber based challenges for leaders, "the explosion of available information creates an environment of mental overload leading to flawed decision making. Failure to master these challenges critically weakens the military instrument of power."[98] Farrell and Lowther warned, "[w]hen thinking about cyber, Airmen often fall prey to misconceptions analogous to those they once encountered from their brethren on the ground."[99] Major General Suzanne Vautrinot, the AF Cyber Commander recently suggested, "[t]he application of cyber

---

[97]Hollis, "USCYBERCOM: The Need for a Combatant Command Versus a Subunified Command," 49.

[98]William B. Osborne, Scott A. Bethel, Nolen R. Chew, Philip M. Nostrand, and YuLin G. Whitehead. "Information Operations: A New War-Fighting Capability," (research paper presented to Air Force 2025, August 1996), viii, http://csat.au.af.mil/2025/volume3/vol3ch02.pdf (accessed December 29, 2012).

[99]Farrell and Lowther, "From the Air: Rediscovering Our Raison D'etre," 75.

capability to enable ground, sea, air, and space operations continue to accelerate, but as with airpower, we should similarly expect cyber to emerge as a strategic alternative."[100]

The contested nature of cyberspace along with thought being put into the role of cyberspace operations in militaries around the world will contribute to interest in questions about the organization of military cyber forces. It is important, then, to understand the process of effecting change in cyberspace organizational structures and to understand the motives of actors that may desire change. In order to do so, focus now shifts to historical examples of organizational change in the US Government and factors that will affect the motives of actors who lobby for or against such changes.

[100]Vautrinot, "Sharing the Cyber Journey," 73.

OBSERVATIONS ON FORMATION OF THE AIR FORCE

> "One of the oldest intuitions-it dates from at least Aristotle-is that conflict between groups is rooted in a clash of interests. Group interests can clash over a wide horizon of valued goods, including claims to social status and privileges"[101]

Taking the first successful ARPANET transmissions in 1969 as a Wright Flyer equivalent, then the existence of the manmade domain of Cyberspace is approaching forty-four years. Like cyberspace, the air domain is relatively young in the history of warfare. Aircraft and the ability to fight in and from the air is just over a century old. Warfare in the cyberspace and air domains has a very short history compared to land and sea warfare, which have been on the scene since early civilization. An examination of the Air Force evolution into a separate service is a useful historic example of how independent organizations dedicated to a "new" form of warfare can evolve from currently existing ones. [102] This section explores relevant observations on organizational change revealed by the series of debates, studies, congressional action, and the two World Wars that occurred in the intervening period. Relevant change factors are then contrasted and compared to current discussions and attitudes to shed light on how and if a separate Cyber Force could come into being.

The first observation the historical record provides is that change requires leadership buy in. During the first two decades of airpower's existence, most advocates arguing for organizational and doctrinal changes were significantly inferior in rank to the leaders opposed to

---

[101]Louk Hagendoorn, Markus Prior and Paul Sniderman, "Predisposing Factors and Situational Triggers: Exclusionary Reactions to Immigrant Minorities," *The American Political Science Review* (Feb 2004): 35-49, http://search.proquest.com.lumen.cgsccarl.com/docview/214413164/abstract?accountid=28992> (accessed December 26, 2012).

[102] Thomas Greer and Herman Wolk authored detailed texts reviewing events from 1907 to 1947 leading to establishment of the US Air Force as a separate service. See Appendix D for highlights of the historical record.

their ideas. This fact meant that despite the quality or validity of the arguments made, they lacked the power and position necessary to bring about change. Their aspirations needed sponsorship from within the Army's existing leadership if they were to gain traction. It is noteworthy that while Congress, an external actor, drove incremental change, Army and Navy leadership frustrated or limited the effects of change in each particular set of debates. Congress, gave voice to the junior Airpower advocates, but as a body based on compromise decision-making, could not produce a consensus powerful enough to overcome military leaders' staunch opposition. This common sense observation indicates that significant organizational change is unlikely until change advocates achieve rank to equal their ideological rivals.

The second observation is that it might take several decades after a new technology or form of war fighting emerges before a sufficient subculture exists to drive radical change. Early leaders of new war fighting spheres are often late adopters of the skills and doctrines associated. Late adopters in this case are individuals whose early career was based on experience in another form of war fighting. While this category of individual may produce staunch advocates, it is less likely those advocates will develop a deep understanding of the capability's potential. Developing effective arguments to back up organizational change will be difficult without a deep understanding of cyberspace. The deep understanding required then will be developed by those who are recruited as new military members and "grow up" practicing the new form of warfare throughout their career. The time to develop home-grown advocates is the approximately 20-30 years it takes the first echelons to reach senior leader ranks. Gregory Rattray, in his book *Strategic Cyber Warfare*, supports this observation as evidenced by citation of at least one study which concluded peacetime doctrinal innovation in military doctrine requires a generation of

officers schooled and committed to waging new forms of warfare develop over a period of up to 20 years.[103]

The third observation is that change is resisted due to human psychology. Social interaction theory states that, "an integral element of individuals' sense of who they are is based on what groups they belong to or identify with…a threat to a group's identity and way of life inherently is a collective threat."[104] Based on this theory, Airmen trying to change existing Army structures and challenge existing theories of war were viewed as a threat to the leaders' group identity. Evidence of this perceived threat was exemplified in the Air Force debates by senior Army and Navy leaders' public pronouncements that aviation advocates were immature, deficient in discipline, and even disloyal early in the debates. Human psychology is a difficult thing to overcome and further suggests that incremental changes will be the norm because they can be absorbed by the psyche without triggering an existential response. Major General Mason Patrick's successful initiatives in the 1920s to garner incremental gains in command authorities, acquisition controls, and doctrine development were an example of changes meeting this threshold criterion.

It must be noted that the current cultural climate is different than existed early in the 20th century and as such leaders may be less threatened by grand change ideas. Advances in the professionalization of the officer corps combined with post-Vietnam lessons may have created senior military leaders that are more open to change ideas which originate from below. Evidence this is the case was detailed by the Tofflers in their review of the process behind the creation of Air-Land warfare doctrine in the 1980s. Generals Starry and Morelli, who were responsible for

---

[103]Rattray, *Strategic Cyber Warfare*, 181.

[104]Hagendoorn, Louk, Markus Prior and Paul Sniderman, "Predisposing Factors and Situational Triggers: Exclusionary Reactions to Immigrant Minorities," 35-49.

developing the doctrine, received assurances from four-star generals in the Army that "disagreement would not be regarded as disloyalty."[105] Further, the author has heard this exact phrase repeated by at least one three-star general during recent interviews. While mental flexibility does not assure adoption of revolutionary ideas, it does provide for a climate that fosters active exploration of potentially controversial topics.

The final observation suggested by the historical record is that a significant event may be needed to drive significant organizational structural change. World War II was the example of this for the formation of the Air Force. More recent examples of significant events leading to major organizational change include the standup of Special Operations Command (discussed in more detail later) after military failures in Iran and Panama, and formation of the Department of Homeland Security after the September 11, 2001 attacks.[106] A significant future cyber event will likely be a necessary, but insufficient variable contributing to whether or not a separate Cyber Force is created. Such an event would force focused attention on the issue and increase leadership will to act in a revolutionary versus incremental way. Social interaction theory is again useful to explain this mechanism. A study by Sniderman, Hagendoorn, and Prior examined mechanisms for and resistance to change within a group regarding a "trigger" event. They found trigger events can both galvanize a core constituency to act on an issue as well as stimulate wider general public support for action. [107] After WWII, President Truman exemplified this concluson when he said:

> Air power has been developed to a point where its responsibilities are equal to those of land and sea power, and its contribution to our Strategic planning is as great. In operation,

---

[105]Alvin and Heidi Toffler, *War and Anti-War*, 59.

[106]See Rattray, *Strategic Warfare in Cyberspace,* 175, for a similar discussion about technology adoption.

[107] Hagendoorn, Louk, Markus Prior and Paul Sniderman, "Predisposing Factors and Situational Triggers: Exclusionary Reactions to Immigrant Minorities," 35-49.

> air power receives its separate assignment in the execution of the over-all plan. These facts were finally recognized in this war in the organizational parity which was granted to air power within our principal unified commands.[108]

Thus, a cyber war or any war with significant action in cybespace may be a precursor to establishment of a separate Cyber Force.

The Air Force experience suggests the likelihood of a separate Cyber Force springing forth in the near future is very unlikely. It also suggests a more probable path will be incremental changes to the current force structures as late-adopter leaders advocate for increased authorities to budget and command and control cyber forces. Further, a separate Cyber Force becomes much more likely after a generation of cyber warriors has advanced to the top ranks and even more so if a significant event occurs, such as a war including significant cyber-attacks with US territory or on US forces. On the other hand, modern organizational constructs may put into question the very feasibility of the idea of a separate service.

[108] Herman S. Wolk, *Toward Independence, The Emergence of the US Air Force 1945-1947* (Government Printing Office, October 1996), 17.

THE POST SEPARATE SERVICE ERA?

The evolution of a separate Air Force occurred in a period where the overall military structure was significantly different then present day. Important differences between past and present conditions qualify limits on the applicability of the Air Force example to the question of a separate Cyber Force. The most noteworthy organizational differences between now and then are establishment of the Department of Defense and creation of the Combatant Commands. Prior to the 1947 National Security Act (NSA), the Army and Navy were independent organizations under US federal code. That independence was gradually removed by putting them and the newly established Air Force under the umbrella of the Department of Defense.[109] During the same post-war period, the issue of establishing a single commander to oversee operations in a theater was addressed and resulted in creation of the Unified Combatant Command system. Even with these two initiatives, however, considerable service rivalry continued to exist over budgeting and mission responsibilities in the post-WWII years. The inability of the services to work effectively together led to successive laws including the DoD Reorganization Act of 1958 and the Goldwater-Nichols Act of 1986, which successively fostered more effective command structures and forced jointness onto the services.

Goldwater-Nichols and the New Jointness

The 1986 Goldwater-Nichols legislation was the result of years of debate and attempts to pass Defense reform legislation. A November 1985 House Armed Services Committee report exploring the "Joint Chiefs of Staff Reorganization Act of 1985," outlined the issues in question that would be addressed in later Goldwater-Nichols legislation:

[109]In reality the NSA established a weak precursor to the Department of Defense called the National Military Establishment.

> The committee concludes that the JCS as structured cannot meet the congressional purpose stated in the National Security Act of 1947: to provide for the unified strategic direction of the combatant forces, for their operation under unified command, and for their integration into an efficient team of land, naval and air forces.[110]

Prior to Goldwater Nichols, the Joint Chiefs of Staff was a committee of peers with limited ability to provide a unified, joint-based voice with which to advise to the National Command Authority. This failure derived from the organizational structure that forced peer Chiefs' to execute compromise-based decision making, which originated during World War II.[111] As the Armed Services Committee pointed out, this is a logical construct in the civilian political arena, but not desirable in the military sphere. In addition to the JCS issues, the unified commanders were viewed to be hamstrung by the power of the services. In essence, combatant commanders had lots of responsibilities and little authority to execute them.[112] Another issue addressed was weakness of the Secretary of Defense. Historically, Congress had acted to minimize the power of the Secretary because it benefited Congress in the political arena. Congress came to recognize that this was fostering deficiencies in defense organizational effectiveness and fostering unacceptable fiscal waste. Goldwater-Nichols was structured to alleviate these issues.

The debates leading up to Goldwater-Nichols mirrored defense organization reform experiences of the past. Debate and passage of the legislation took nearly three years. During that time, Congress plus retired generals seeking the changes were pitted against the majority of

---

[110]House Armed Services Committee, *Joint Chiefs of Staff Reorganization Act of 1985*, 99th Cong., 1st sess., 1985, Rep 99-375, 11, https://digitalndulibrary.ndu.edu/cdm4/document.php?CISOROOT=/goldwater&CISOPTR=868&CISOSHOW=831 (accessed 9 April 2013).

[111]James R. Locher III, "Has it Worked? The Goldwater-Nichols Reorganization Act," *Naval War College Review* 54, no. 4 (Autumn 2001): 95-115. http://www.usnwc.edu/getattachment/744b0f7d-4a3f-4473-8a27-c5b444c2ea27/Has-It-Worked--The-Goldwater-Nichols-Reorganizatio (accessed 24 April 2013).

[112]Ibid, 167.

sitting four-star Service Chiefs and the JCS Chairman.[113] It took external intervention to drive significant organizational change. In addition, significant events, this time in the form of military failures, were largely cited as impetus for Congress to act decisively on the Goldwater Nichols legislation. These experiences reinforce the change process trends derived from the Air Force example.

Review of the results of Goldwater-Nichols enactment over the last 27 years, raises the question whether a separate Cyber Force is any longer feasible or even required in the future. The first reason for this is that the slow mechanism of externally mandated organizational change may no longer be necessary. Since 1986, iterations of the Unified Command Plan (UCP) have created and eliminated many combatant command structures as the times and security conditions have required. The ability to make such changes lies in the increased power Goldwater-Nichols gave the Secretary of Defense. Unlike previous eras, the Secretary can drive organizational change with much less requirement for consensus, which increases the flexibility of military organization in the US. In addition, Combatant Commanders in the process of executing military taskings around the world, have pushed (or forced) ever increasing jointness amongst the services, resulting in the high level of inter-service operability today. The increased ability and willingness to operate jointly, along with the ability to create organizational structures within the scope of the Unified Command Plan may alleviate any "need" to create a separate Cyber Force.

SOCOM – Rise of the Service-Like COCOM

The specific example that casts a shadow on the feasibility or need of a separate Cyber Force is Special Operations Command (SOCOM).[114] While Defense reform was under debate

---

[113]Ibid, 167.

[114]Andrew Feickert, "The Unified Command Plan and Combatant Commands: Background and Issues for Congress," Congressional Research Service (July 17, 2012): 17,

from 1981-1986, legislators were also examining the command and funding issues for Special Operations Forces (SOF). Legislative inquiry testimony painted the picture of services with little interest in special operations, a DoD not adequately preparing for future threats that SOF could address, and of SOF designated funds routinely siphoned off by the services for other purposes. These observations convinced legislators that a more efficient organization and direct chain of command was necessary.[115] In addition, mission failure in the 1980 Iranian Hostage Rescue attempt and ineffective use of SOF leading to high casualty rates during the 1983 Invasion of Grenada provided traumatic evidence that current organizational paradigms were inadequate. To resolve the issues, SOCOM was created in the 1987 Cohen-Nunn amendment to the 1986 Goldwater-Nichols Act.[116] It should be noted, that like formation of the Air Force and Goldwater-Nichols legislation, formation of SOCOM was resisted by top military leadership. A CRS report noted that Admiral William J. Crowe, the JCS Chairman, led opposition and favored a special operations forces command led by a three-star general. Congress rejected this proposal and established the SOCOM commander as a four-star so as to have equal footing with the Service Chiefs.[117]

The unique construct of SOCOM arguably created a sixth "service-like" component. The Nunn-Cohen amendment effectively grafted many roles and authorities normally associated with

---

http://www.fas.org/sgp/crs/natsec/R42077.pdf (accessed December 30, 2012).

[115]Ibid, 1.

[116]Bryan D. Brown,"U.S. Special Operations Command: Meeting the Challenges of the 21st Century" *Joint Forces Quarterly* 40 (May 2006), http://www.army.mil/professionalWriting/volumes/volume4/ may_2006/5_06_1.html (accessed 4 February 2013).

[117]Feickert, "The Unified Command Plan and Combatant Commands: Background and Issues for Congress," 16.

the Services onto the Unified Command Plan construct.[118] The SOCOM organizational structure set a precedent under the umbrella of the UCP and at the same time solved several problems and avoided several pitfalls that would be associated with standing up a new service. First, it avoided the caustic independence question with its associated issue of carving chunks (people, equipment, capabilities, etc.) out of the existing Services. Second, it solved the unity of command problem for forces that arguably did not have a lead service and also provided a Secretary-like civilian oversight position. Third, it preserved connection between the existing Services and their Special Operators, fostering retention of cultural bonds, but also saddling the Services with most basing and equipment provisioning responsibilities. Finally, even though the creation of SOCOM required legislative action, the precedent set by establishing a Service-like entity within the UCP process effectively transferred the ability to create similar organizational structures to the Executive branch. Congress will still have significant power to shape such organizations, but establishment and growth of an organization over a number of years may be the equivalent of an Executive branch fait-accompli' for issues Congress would previously address. The establishment of CYBERCOM, discussed in the next section, which though a Sub-Unified Command at present was established by Secretary of Defense order rather than Congressional action, just as the SOCOM example suggested would be the case.

---

[118]This is acknowledged in the JP 1 statement "USSOCOM is unique among the combatant commands in that it performs certain Service-like functions…"(III-10). SOCOM service like functions listed in JP 1: (1) Organize, train, equip, and provide combat-ready special operations forces (SOF) to the other combatant commands and, when directed by the President or SecDef, conduct selected SO, usually in coordination with the GCC in whose AOR the SO will be conducted. USSOCOM's role in equipping and supplying SOF is generally limited to SO peculiar equipment, materiel, supplies, and services. (2) Develop strategy, doctrine, and tactics, techniques, and procedures for SOF, to include psychological operations (PSYOP) and civil affairs (CA) forces. (Note: Joint doctrine is developed under the procedures approved by the CJCS.) (3) Prepare and submit to the SecDef program recommendations and budget proposals for SOF and other forces assigned to USSOCOM. JP 1, III-10-12.

SOCOM also reinforces the observation that success in significant national events provides the leaders of sub-organizations the clout to drive through organizational change. In recent years SOCOM responsibilities and authorities have grown beyond those originally established. After the September 11, 2001 attacks, SOCOM was given responsibility to synchronize DoD planning and act as the lead COCOM for planning and operations against terrorists across the globe.[119] Success in this endeavor, most visibly represented by the killing of Osama Bin Laden, has provided the SOCOM Commander with considerable credibility and political clout. Recently, Admiral McRaven, the current SOCOM Commander, effectively leveraged his influence to seek and apparently gain increased authorities including COCOM authority over the Theater Special Operations Commands (TSOC). The TSOCs will now be Sub-Unified commands under SOCOM where they were formerly aligned under the Geographic Combatant Commands (GCCs). Interviews with SOCOM staffers indicated that original resistance to the authorizations may have been partly based on fear that SOCOM was trying to create a sixth service.[120] The fact SOCOM was granted the authorities requested reinforces the observation from the development of the Air Force case about clout and credibility gained from success in major military operations being a factor in driving through organizational changes.

The test of time is now required to determine whether the arrangement satisfies the command and control goals of the SOCOM commander and makes worldwide SOF training, equipping, and employment more efficient and SOF forces more effective. It will be interesting to see if these new authorities are indeed just a fine tuning of the current force structures or whether

---

[119]Feickert, "The Unified Command Plan and Combatant Commands: Background and Issues for Congress," 15.

[120]Author Interviews at SOCOM, December 2012 and SOCPAC, February 2013. The author considers the Coast Guard the fifth Service.

fears of a sixth service push prove to be grounded. In either case, the ability of the SOCOM Commander to successfully lobby for increased authorities will increases the appeal of SOCOM as "the model" for those interested in the separate Cyber Force question.

Currently, there are several indicators in the cyberspace literature that suggest the SOCOM model does appear to be the favored organizational template for future cyber force structures. First, before the standup of USCYBERCOM some of the literature lamented that there was no lead service for cyberspace operations. Second, a 2011 article suggested that cyber forces may parallel special operators to such an extent that USCYBERCOM should be aligned under SOCOM.[121] Third, cyber leaders are advocating acquisition reform necessary to match processes with the rapid development cycle of information technology and the SOCOM model of acquisition authorities may be a more feasible path to this goal than DoD-wide acquisition reform. Finally, several recent monographs have advocated SOCOM-like authorities and capabilities for CYBERCOM including, elevation to fully Functional COCOM status, acquisition authority for cyber unique programs, and evolution of the cyber capabilities within the Geographic COCOMs to achieve TSOC-like "organic" cyber capabilities. The push for CYBERCOM to evolve in the image of SOCOM is logical as: it allows use of an established model that is much less contentious than a Separate Service argument and authorities can be lobbied for in increments which fit the "rate of change" environment within DoD. If CYBERCOM does evolve along the SOCOM model in the out years, it will greatly reduce the likelihood elements within the cyber community would be compelled to forward the radical idea of creating a separate Cyber Force.

---

[121]Stew Magnuson, "Do Cyberwarriors Belong at Special Operations Command," *NationalDefenseMagazine.org,* August 2011, under "Cybersecurity," http://www.nationaldefensemagazine.org/archive/2011/August/Pages/DoCyberwarriorsBelongatSpecialOperationsCommand.aspx (accessed 23 April 2013).

CYBER FORCES ORGANIZATIONAL STRUCTURE

> "The work of organization is never done, and the structure has to be continually adapted to new and anticipated conditions."[122]
>
> – Ralph Cordiner, *New Frontiers for Professional Managers*

If designating cyberspace a domain is a force organizing concept, then the current cyber force structure is the result of that initiative. It is necessary to examine this force structure to determine whether it effectively addresses national military goals in cyberspace. If the current organizational construct proves effective, then there will be diminished impetus to create a separate Cyber Force. This section begins by examining in detail US Cyber Command (USCYBERCOM), which was created by 2009 Secretary of Defense Memorandum.[123] The evolution of Cyber Command and military cyber organization efforts is then examined. The section concludes with the exploration of a model for organizational change that suggests the young age of USCYBERCOM will detract from any push for a separate Cyber Force in the near term.

US Cyber Command

The organizational structure of cyber forces mandated in 2009 has been evolving since the early 2000s. Richard Clarke, who served four Presidents in the White House, gives an insider's account of the formation of the current construct in his book *Cyber War*. In an effort to protect defense networks, a Joint Task Force for Computer Network Defense was created in 1998, assigned to USSPACECOM, and rolled into USSTRATCOM in 2002 when USSPACECOM was

---

[122]Ralph J. Cordiner, *New Frontiers for Professional Managers* (New York: McGraw-Hill Book Company, 1956), 54.

[123] See Appendix E for a review of cyberspace responsibilities across the US Government and within DoD.

dissolved.[124] As computer attacks against DoD became more sophisticated and frequent, the vulnerability of the US to such activities emerged in the public and policy consciousness and there were calls to place greater emphasis and visibility on cyber operations. One outcome of efforts to address vulnerabilities has been an evolving defense organizational structure. According to Clarke, attempts by the Air Force to create a Cyber Command in 2007 created rivalries between the services over who would control the future of US cyber operations.[125] Eventually, a joint command structure was agreed upon, but the command developed was a compromise tempered by past experiences.

One of the experiences that affected the debate was the rise and fall of USSPACECOM. USSPACECOM had been a functional Combatant Command from 1985 to 2002. In its heyday in the 1990s, the importance of the space domain and space operations were discussed in similar terms as cyberspace and cyberspace operations have been over the last decade. At one point in 1998, the USSPACECOM Commander lobbied for the Functional Combatant Command to be elevated to Geographic Combatant Command status.[126] This attempt failed, however, and four

---

[124] The declassified 2002 Unified Command Plan tasks USSTRATCOM (item 21j.) with "integrating and coordinating DoD information operations (IO) (currently consisting of the core IO capabilities of computer network attack (CNA), computer network defense (CND), electronic warfare (EW), operations security (OPSEC), military psychological operations (PSYOP), and military deception (MILDEC)) that cross geographic areas of responsibility…" from http://www.bits.de/NRANEU/others/strategy/UCP-1-2003.pdf (accessed April 13, 2013).

[125]Clarke and Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, 36.

[126]Mark A. Morris,"Who Will Command The High Ground? The Case For A Separate Area of Responsibility for Space" (monograph, Air War College, 1998), 5. There is at least one other monograph on this topic published in the same year by Keith McDonald. The two papers come to opposite conclusions regarding making SPACECOM a GCC using starkly different reasoning. Ultimately the demise and absorption of SPACECOM into STRATCOM occurred. Morris' paper is interesting because he couches discussion of the space domain in much the same way cyberspace is discussed today, "integral to US way of life, emerging as a new battlefield, etc." McDonald's paper includes hand wringing about the danger of weaponizing space,

years later in 2002, USSPACECOM was eliminated and its functions were merged into USSTRATCOM. Officially this occurred to, "eliminate redundancies and streamline decision-making."[127] Clarke suggests the change happened because "no government had enough money to do much in space" and the concept of space war fighting was viewed as a passing fad.[128] Memory of the rise and fall of USSPACECOM likely caused policy makers to have reservations when considering the form to give a new strategic cyberspace organization.

Another contributing factor in the organizational debate was the historical involvement in cyberspace by the National Security Agency (NSA). Two former NSA Chiefs, concerned that the military would reinvent the wheel on capabilities the agency had spent decades developing, weighed in to affect the organizational structure. The compromise organization that evolved from the debates was US Cyber Command, designated a Sub-Unified Command under USSTRATCOM. The commander, a four-star general, was dual hatted to serve as the NSA Director also.[129] Clarke ultimately gave credit for the compromise that evolved to former Secretary of Defense Robert Gates who announced the formation of USCYBERCOM in a June 2009 memorandum.[130]

---

interesting in light of the Chinese ASAT tests which occurred in January 2007.

[127]U.S. Department of Defense, *2002 Year In Review* (December 31, 2002), 10, http://www.dtic.mil/docs/citations/ADA475302 (accessed 28 December 2012).

[128]Clarke and Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, 35, 37. In 2011, the UCP removed responsibilities for IO (also Mil Deception and Ops Security) from STRATCOM and put it with the JCS.

[129]The linkage of signals intelligence necessary to anticipate intrusions to the Defense Department's collective cyberdefense capabilitites was one of the most important reasons for the creation of Cyber Command according to former US Deputy Secretary of Defense William J. Lynn III. The NSA Director was previously a three-star general

[130] U.S. Government Accountability Office, *Defense Department Cyber Efforts: More Detailed Guidance Needed to Ensure Military Services Develop Appropriate Cyberspace*

USCYBERCOM was established May 21, 2010 and declared fully operational on October 31, 2010.[131] The current Commander is General Keith Alexander. Cyber Command is co-located with the NSA at Fort Mead, Maryland. USCYBERCOM is responsible for planning, coordinating, integrating, synchronizing and directing activities to operate and defend DoD information networks, and to conduct full spectrum cyber operations when directed.[132] The command was established with three missions: lead protection of all defense networks and support of military and counterterrorism missions with operations in cyberspace, establish a clear and accountable way to marshal cyber warfare resources from across the military, and work with interagency and external partners.[133]

Evolution of Cyber Force Structures

> "For years, and especially since DoD proposed to establish a Cyber Command, the Armed Services Committee has emphasized the lack of effective, mature policy, strategy, rules of engagement, doctrine, roles and missions, and command and control arrangements that are so critical to managing this vital but complex new domain. Progress in this area has been slower than we desired, but appears to be picking up steam." - Senator Carl Levin's opening statement for a Senate Armed Services Committee hearing on US CYBERCOM, March 12, 2013.

Capabilities (U.S. Government Accountability Office, May 2011): 3, http://cryptome.org/0004/gao-11-421.pdf (accessed 3 April 2013).

[131]Feickert, "The Unified Command Plan and Combatant Commands: Background and Issues for Congress," 20. See Appendix F for a listing of the Service Cyber Components which were also directed in the Secretary of Defense Memorandum.

[132]Gina Cairns-McFeeters, "United States Cyber Command," *The CIP Report* 9, no. 7 (January 2011): 5-6, 20, http://cip.gmu.edu/archive/CIPHS_TheCIPReport_January2011_Cybersecurity.pdf (accessed 23 August 2012).

[133]Lynn, "Defending a New Domain: The Pentagon's Cyberstrategy." The 2009 Memorandum also mandated the standup of Service Component Cyber Commands. See Appendix F for details on the service cyber commands.

The evidence makes it clear that joint and interagency cooperation has been a key element of cyberspace force structures since Secretary Gates published the memorandum establishing CYBERCOM and the Service cyber components in 2009. Dual hatting the CYBERCOM Commander as the NSA director ensured unity of command and tie in of the nation's cyber intelligence capability with developing Cyber Command operational capabilities. Additionally, before Cyber Command was operational, the DoD and DHS signed a memorandum of agreement (MOA) in order to "increase interdepartmental collaboration in strategic planning for the Nation's cybersecurity, mutual support for cybersecurity capabilities development, and synchronization of current operational cybersecurity mission activities."[134] The MOA directed CYBERCOM, NSA, and DHS each to consider requests for support from the other and established liaison elements within each organization to foster open communication channels between them. The MOA was given impetus for action by also establishing an oversight committee at the DHS and DoD Deputy Secretary level.

In addition to agencies tasked with cyberspace responsibilities, outside elements have fostered joint and interagency cooperation through continual analysis and commentary on the state of cyber policy and organization. For example, Government Accountability Office and RAND Corporation studies from 2010 suggested that cyberspace roles across the government had yet to be hammered out. Around the same period, former NSA director Ken Minihan expressed belief that current cyber war planning lacked a national-planning system to get all organizations working on the same page, vice doing what each organization "wants" to do.[135] A slew of recent

---

[134]"Memorandum of Agreement Between the Department of Homeland Security and the Department of Defense Regarding Cybersecurity" (October 13, 2010): 1, http://www.dhs.gov/xlibrary/assets/20101013-dod-dhs-cyber-moa.pdf (accessed 9 April 2013).

[135]Clarke and Knake, *Cyber War: The Next Threat to National Security and What to Do*

Congressional testimony and public statements from General Alexander and others indicate that a lot of work has been done to address such findings and *cybersecurity* lanes may be much clearer than three years ago.

In May 2012, the Joint Staff Transitional Command and Control Concept of Operations was approved and established Joint Cyber Centers (JCC) and Cyber Support Elements (CSE) in the Geographic Combatant Commands.[136] The CONOP defined baseline command relationships, missions, functions, and tasks for the JCC and CSE teams. In addition, a lead Service Component was assigned responsibility for supporting each of the GCC's cyberspace efforts.[137] Cyber Command also issued Operational Directive 12-001 in April 2012, which granted direct liaison authority to the Service Components to work with joint, combined, interagency, and commercial entities to plan and execute assigned cyber tasks.[138] The effectiveness of the JCC/CSE structures remains to be seen. Interviews with staff officers in several COCOMs indicated that the

---

About It, 43.

[136]Suzanne El Sanadi, "Protecting the Grid: DoD Fortifies Itself Against Threat of Cyber Attacks," The Foundry Blog, entry posted June 14, 2012, http://blog.heritage.org/2012/06/14/protecting-the-grid-dod-fortifies-itself-against-threat-of-cyber-attacks/ (accessed 9 April 2013).

[137]House Armed Services Committee, *Statement of MGEN Suzanne M. Vautrinot Commander Air Forces Cyber 25 July 2012*, 8, http://armedservices.house.gov/index.cfm/hearings-display?ContentRecord_id=c0de6683-61a9-4b83-b443-8a8c45ff5009&Statement_id=99f81c1d-b026-455e-b58d-3288a8c57a12&ContentType_id=14f995b9-dfa5-407a-9d35-56cc7152a7ed &Group_id=41030bc2-0d05-4138-841f-90b0fbaa0f88&MonthDisplay=7&YearDisplay=2012 (accessed 12 September 2012).

[138]House Armed Services Committee, *Statement of VADM Michael S. Rogers Commander, United States Fleet Cyber Command Before the Emerging Threats and Capabilities of the House Armed Services Committee on 25 July 2012*, 3, http://armedservices.house.gov/index.cfm/hearings-display?ContentRecord_id=c0de6683-61a9-4b83-b443-8a8c45ff5009&Statement_id=7fc85bab-d453-4e30-947e-03bb1a48f5c9&ContentType_id=14f995b9-dfa5-407a-9d35-56cc7152a7ed&Group_id=41030bc2-0d05-4138-841f-90b0fbaa0f88&MonthDisplay=7&YearDisplay=2012 (accessed 12 September 2012).

organizational directive lacked the accompanying personnel to fill out the teams.[139] In addition, a recent article discussing the concept cited internal resistance and inter-command frictions associated with the new organizing construct.[140] Such turbulence, as discussed shortly, is a natural part of standing up new organizations and time may be the essential element required before effectiveness of the JCC/CSE concept can be adequately measured.

Personnel sourcing issues may already have been addressed however, evidenced by recent announcement of the formation of missionized Cyber Teams. In January 2013, Cyber Command outlined plans to form three types of Cyber Teams. First, a Cyber National Mission Force consisting of 13 teams will be responsible for defending the nation against national-level threats. General Alexander, in Senate testimony, stated these teams will be able to conduct offensive operations in the course of defending the US, indicating they will have authority to act in networks outside of the US.[141] It appears these teams will be closely integrated with the DHS and the FBI and focus on US critical infrastructure (financial system, transportation system, power generation, etc.).[142] Second, a Cyber Combat Mission Force consisting of 27 teams will be assigned to and under operational control of individual combatant commanders to support offensive cyber planning. Logically these teams would flesh out the JCCs/CSEs. Third, a Cyber

---

[139]Author interviews with EUCOM, AFRICOM, CENTCOM, SOUTHCOM, PACOM, and TRANSCOM staff members in 2012 and 2013.

[140]Zachary Fryer-Biggs, "U.S. Regional Commanders Get New Cyber Muscle," *Defense News*, June 9, 2012, http://www.defensenews.com/apps/pbcs.dll/article?AID=2012306090001 (accessed 9 April 2013).

[141]Senate Armed Services Committee, "Oversight: US Strategic Command and US Cyber Command."

[142]It should be noted here that senior military officials frequently cite intent to leverage the NSA's Title 50 responsibilities, the FBI's Title 18 responsibilities, and the National Guard's Title 32 responsibilities when necessary to allow military cyber teams to be employed on networks inside the US.

Protection Force will operate and defend DOD's information environment. Mention was also made of a fourth set of direct support teams but the report lacked further elaboration.[143] Articles discussing these teams also report that Cyber Command will expand from 900 personnel to 4,900 personnel.[144] This personnel expansion has lacked context in media reports so far. Reporters have concluded that it constitutes an increase in the number of cyber forces, while General Alexander's Senate testimony indicated the extra 4,000 personnel would come from the Service Components. It will take three years to stand up the full complement of teams outlined above, with 1/3 completion targeted for each of the years 2013-1015. Furthermore, According to Gen Alexander, command relationships and information passing processes have been worked out between COCOMs and Service Chiefs, but he said there was more work to be done as the teams come on line.[145] It will take years before this new organizational construct can be analyzed for effectiveness and efficiency. Periodic examination of how resources are being applied over the next several fiscal years will be perhaps be the most readily available indicator of success or failure of this organizing concept, but the evidence suggests an active evolution of cyber force structures and command relationships which will likely minimize internal motivation to lobby for a separate Cyber Force.

"Up and out" organizing activity has accompanied the "down and in" initiatives detailed above. According to statements by General Alexander, lanes have been established for

---

[143]Cheryl Pellerin, "Cybercom Builds Teams for Offense, Defense in Cyberspace," *American Forces Press Service*, March 12, 2013, http://www.defense.gov/news/newsarticle.aspx?id=119506 (accessed 9 April 2013).

[144]Ellen Nakashima, " Pentagon to Boost Cybersecurity Force," *Washington Post*, January 27, 2013, http://articles.washingtonpost.com/2013-01-27/world/36583575_1_cyber-protection-forces-cyber-command-cybersecurity (accessed 17 March 2013).

[145] Senate Armed Services Committee, "Oversight: US Strategic Command and US Cyber Command," 53:40.

USCYBERCOM, NSA, DHS, the FBI, and partners like the National Institute for Standards and Technology.[146] In March 2013 Senate testimony, he noted no single private or public entity possesses the complete set of authorities to detect, prevent, and mitigate a cyber attack. Since no single agency can completely defend the nation in cyberspace, an active and effective working relationship among the Executive Departments and Agencies is a necessary requirement. If the relationships prove productive, then there will be little external impetus for radical organizational changes. However, should these intra-government relationships breakdown or fail to effectively integrate information, planning, and operations (likely signified by failure in the face of a major cyber attack on the US), then radical organizational change could gain momentum. The question arising from this discussion is how long is an appropriate time to give a new organization before considering alternatives.

The Time Factor

Stewart Baker, former DHS Assistant Secretary for Policy, outlined a development model for creating new government organizations during testimony before the Senate in 2009. [147] At the time Congress was looking into establishing a National Office for Cybersecurity, under a new Assistant to the President, which would take over DHS' relatively new responsibility for cross-government coordination of cyber issues. He outlined three stages that occur in the process of creating a new government agency. The first stage is a change proposal based on flawed current organizations or failures such as the 9/11 attacks that led to creation of DHS. The second stage is envisioning a new organization, which includes temptation to give it great responsibility, since as

[146]Pellerin, "Cybersecurity Involves Federal, Industry Partners, Allies."

[147]Baker helped start the Education Department in the 1970s and started up the DHS Office of Policy.

a purely conceptual construct it has no flaws and has never failed. The third stage consists of formation of the new organization, where imagined productivity initially suffers due to administrative realities of hiring personnel, setting up offices, and establishing contracts.[148] In summary, Baker implies that it takes a period of many years for a new organization, especially a large government organization, to achieve appreciable effectiveness and he insinuates that tampering with organizational structures too often, leads to a continuous cycle of inefficiency. The fact that CYBERCOM is "picking up steam," combined with Baker's hypothesis that new organizations need time to achieve effectiveness, suggest it may be prudent to wait the better part of a decade (absent a shocking failure) before anything as significant as a separate Cyber Force be considered as an organizational alternative.

MOTIVATIONS FOR ORGANIZATIONAL CHANGE

This section explores motivations that would drive actors to seek a separate Cyber Force. It begins with examination of the effect power of identity has on motivating those who would advocate to establish a separate Cyber Force. It then turns to examination of organizational effectiveness. If cyber forces in the current structure are demonstrating characteristics of effective organizations, there will be diminished motivation for radical organizational change both internally and externally.

Personal Motivations

The role of shared identity of cyber forces within the services will contribute to whether or not motivation for a separate Cyber Force develops. Carl Builder in *The Masks of War:*

---

[148]Senate Committee on Homeland Security and Governmental Affairs, *Statement of Stewart A. Baker, Partner Steptoe and Johnson LLP Before the Committee on Homeland Security and Governmental Affairs* (28 April 2009), http://www.hsgac.senate.gov/download/042809baker (accessed 12 September 2012).

American Military Styles in Strategy and Analysis explored the power of identity in the Services. Builder points out that a trait of high functioning organizations is a shared sense of identity and purpose, which facilitates difficult decision-making.[149] The implications of Builder's assertion is that if the soldiers, sailors, airmen, and marines in the service cyber components continue to identify with their respective services above identifying as Cyber Warriors, then current cyber force structures will likely continue. On the other hand, development of a Cyber Warrior identity over service identity will motivate Cyber Warriors to seek establishment of a separate Cyber Force. The historical record of the path to a separate Air Force serves as example of such divergence in identity and purpose. Builder's argument further suggests that such a divergence in identity might occur if cyber forces continually end up on the losing side of the difficult decision-making. The failure of Cyber Warriors to gain promotion to higher leadership positions, rejection of cyber resourcing priorities, and rejection of cyber doctrinal innovation are examples of losses that could cause divergence in identity and provide motivation to lobby for a separate Cyber Force.

The motivation to pursue a separate Cyber Force due to identity divergence or frustration of ambition will, however, be minimized if the current force structure is able to address such concerns. The creation of CYBERCOM under the Unified Command Plan has the potential to do just this, and once again, SOCOM is the example of why. Under SOCOM, Special Forces personnel have an organization with which to identify their special skills and which also advocates for promotion, resourcing, and doctrinal aspirations. The SOCOM Commander has resourcing and doctrinal authorities, and is seeking more authority to manage Special Forces

[149]Carl H. Builder, *The Masks of War: American Military Styles in Strategy and Analysis* (Baltimore: The Johns Hopkins University Press, 1989): 36.

promotions.[150] Special Forces personnel can in effect maintain both service and Functional identities without being forced to choose one and reject the other. If CYBERCOM develops along similar lines to SOCOM, then motivation for an independence movement among cyber forces may be minimized. Identity is an important motivator, but individuals will also be motivated by the effectiveness of the organization they identify with. Since people will largely associate with institutions for positive reasons, it is logical that effective organizations will foster positive association. We now turn to examination of the effectiveness of current cyber force structures.

Organizational Efficiency Motivations

Cyberspace is a manmade domain and based on the development of information technologies (IT). As such, organizations that are concerned with cyberspace operations will very much be IT oriented and must effectively develop IT capabilities to maximize operational capabilities in cyberspace. Gregory Rattray in *Strategic Warfare in Cyberspace*, asserts that in order to develop technological capability, organizations need to have the following characteristics: a supportive institutional environment, demand-pull motivation, managerial initiative, technological expertise and learning capacity.[151] As an indicator of future potential, let us examine recent literature and events to determine whether the elements of the current cyber force structure are displaying these characteristics.

When considering whether or not the separate Cyber Force idea has merit, the question of a supportive institutional environment must be addressed at the COCOM and service levels. If at these levels there is a lack of institutional support, then the subordinate cyber organizations will suffer for resources and advancement opportunities. Public statements by General Keith

---

[150] Author interviews with SOCOM staff, December 2012.

[151]Rattray, *Strategic Warfare in Cyberspace*, 227.

Alexander indicate that cyberspace issues receive focused attention at the four-star general level across the services, which suggests institutional support. In addition to focus, The *DoD Budget for Fiscal Year 2013* indicates that resources are being prioritized towards cyberspace with the assurance, "the Budget sustains and enhances all aspects of DOD's cybersecurity capabilities."[152] In interviews, DoD Chief Information Officer (CIO) Teresa Takai, stated that $37 billion of the defense budget is targeted to information technology including $3.4 billion for *cybersecurity* efforts and $182 million for Cyber Command.[153] The enactment of sequestration in March 2013 will test budgetary resolve by DoD institutions to prioritize funding for cyberspace concerns. A significant issue related to shrinking budgets is the projected reduction in manpower across the services. Because cyber forces are sub-elements of the services, increasing or maintaining numbers of personnel in cyberspace career fields will come at the expense of other branches in each of the services. How the services choose to make reductions of personnel within their branches will indicate the level of support for cyber forces going forward. Significant negative trends in cyber force funding or manning-levels will foster independence motives within the Service Cyber Components.

Rattray defines demand-pull motivation as the internal motivation of organizations to make the substantial effort and organizational changes necessary to quickly and successfully drive new technologies.[154] Military support and funding to develop the first large scale digital

---

[152]U.S. Department of Defense, *Overview, Fiscal Year 2013 Budget Request* (Office of the Under Secretary of Defense (Comptroller) / Chief Financial Officer, February 2012), 29, http://comptroller.defense.gov/defbudget/fy2013/FY2013_Budget_Request_Overview_Book.pdf (accessed 29 January 2013).

[153]Pellerin, "DOD Devleops Cybersecurity Rules of Engagement."

[154]Rattray, *Strategic Warfare in Cyberspace*, 175.

computers and computerized networking are examples of this characteristic.[155] The rapid adoption and dominance of the information technology sector by private enterprise brings into question whether military organizations will suffer due to a mismatch of demand-pull compared to the civilian sector. For example, while development of networked radios, blue force tracker programs, etc., indicate continued emphasis to harness information technology in the battlespace, the DoD has been late to adopt mobile and wireless technology for military applications. The rapid creation-destruction cycle in private industry appears to be outpacing the US Military's ability to match or stay ahead of it.[156] Such a mismatch in demand-pull may allow adversaries (both state and non-state) to gain advantage in cyberspace. There are, however, signs of demand-pull motivation in current military cyberspace organizations. Examples of this behavior include the previously mentioned DARPA Plan X, exploration into "big data" applications, and the emphasis on developing automated network defenses.

Rattray also asserts that doctrinal flexibility is the military aspect of the demand-pull characteristic.[157] On this topic, whether current organizations, especially USCYBERCOM, exhibit the trait remains to be seen. Currently, the services and the Joint Staff have published Information Operations doctrine that covers some cyberspace operations topics. The Air Force published Cyberspace Doctrine in 2010, last updated in November 2011. News reports indicate that Joint Cyberspace Doctrine has been in development for several years, but is yet to be approved and released. The evidence suggests that current cyber organizations are in fact

---

[155]Ibid, 175.

[156]Perhaps this is inevitable as acquisition programs in the military are governed by Congressional budget negotiations which circumvent the private sector's thrive or die environment. Congress is an indirect representative of "self-interest" and as such acts slower than entities who act in their own direct self-interest.

[157]Ibid, 176.

demonstrating some demand-pull characteristics. What is not clear is whether in future years, the current organization construct will be able to adapt quickly enough to outpace potential adversaries.

Managerial initiative is about leadership. In the realm of technology adoption it includes providing a vision and fostering a culture that can adapt to a rapidly changing environment. This includes the willingness to allocate resources to new technologies, flattening organizations and empowering outside connections, fostering an innovative culture, and ensuring acquisition of experiential knowledge (not just hardware).[158] Once again, the critical examination of this topic will lie in the interaction between Service Cyber Component Commanders and their superiors in the service chain of command. The following quote illustrates the issue:

> I still twitch when I say cyber. I'm a believer. I'm just not sure we know exactly what we're doing in it yet and until we do, I'm concerned it's a black hole…..we have a lot of people in this discussion who don't really know what they're talking about. I know because they're all like me…I haven't figured out what an IP address is yet. In 30 years you'll have experts making these decisions. Right now you've got idiots helping make these decisions.[159]

This represents the challenge Cyber Component Commanders will face in that, as subordinate branches, cyber organization leaders will be competing for resources, pushing ideas, and advocating force structures that may be completely outside the comfort zone of the Service Chiefs. The true test of managerial initiative will come at that level. If Service Chiefs retreat to the defensive mindset of rejecting concepts either because they do not fully trust the source or do not fully understand the concept, then cyberspace capabilities may founder.

---

[158]Ibid, 176.

[159] General Mark Welsh, "Comments to Air Force Association Convention" (18 September 2012).

Technological expertise and learning capacity in an organization are human issues. They revolve around building or recruiting personnel with the mix of skills necessary to operate in cyberspace and continuing education initiatives. Expertise thus comes with both personnel and training costs. The more specialized the expertise, the more training required and the more competition for talent. Compounding military leaders' problem is the fact many cyberspace skills are readily transferrable to the private sector.[160] Congressional testimony indicates strong awareness of these issues by military leaders. There is demonstrated concern over the ability to compete with the private sector in both salary and culture categories.[161] Existing proposals to address these concerns include educational research and scholarship programs, pay and bonus structures to make salaries competitive, the placing of cyber forces into National Guard and Reserve units in order to capitalize on private sector expertise, and the possibility of structuring cyber forces to include a significant number of DoD civilians.[162] In addition to recruiting and force shaping initiatives, the services have or will establish cyberspace-training regimes. As an example, the Air Force has established undergraduate, intermediate and advanced cyber training courses.[163] Congressional testimony suggests military cyber leaders are focused on developing technological expertise and learning capacity within the current cyber force structure. Looking forward, examination of whether Service Components are able successfully to recruit, train, and retain a competent cyber workforce will demonstrate whether the current cyber force structures

---

[160]Ibid, 222.

[161]Feickert, "The Unified Command Plan and Combatant Commands: Background and Issues for Congress," 23. Cyber leaders have expressed concern that personnel with high-end cyberspace skills may not "fit" with military culture.

[162]House Committee, *Statement of MGEN Suzanne M. Vautrinot,* 1-12.

[163]These courses are Undergraduate Cyber Training (UCT), mission qualification training (conducted at units), and the Cyber Weapons Instructor Course at Nellis AFB, NV.

are effectively harnessing technological expertise and learning capacity. Negative indicators, which would suggest an alternative be sought, include continuous inability to meet cyber manning numbers and/or resorting to reliance on contractors to provide military cyber capabilities. One important characteristic of cyberspace expertise is knowledge of the possibilities and limitations of the technologies and operations in and through the domain.[164] It will be important for the Service Components to maximize this expertise both to provide the best military cyberspace options to Joint Force Commanders and to compete effectively for resources in the coming constrained environment.

The relatively young age of the current cyber force structure once again precludes absolutes in the analysis of effectiveness of the construct. The evidence as reviewed in this section, however, indicates that organizations appear to be developing or exhibiting the five characteristics necessary to develop technological capability. If cyber force elements continue to exhibit these characteristics, then by Rattray's framework, they will successfully build cyberspace capability, which would negate internal and external motivation to create new organizational structures such as a separate Cyber Force.

CONCLUSION

The DoD declaration of cyberspace as a war fighting domain is an organizing concept. The military cyber force organizational structure created by Secretary of Defense Memorandum (June 23, 2009) consists of USCYBERCOM, a functional Sub-Unified Command under USSTRATCOM, and Cyber Components in each of the services. The current force structure generates the question of why, if cyber forces are to be organized like land, sea, and air forces, will there not be a separate Cyber Force? This question is difficult to resolve because it can

[164]Rattray, *Strategic Warfare in Cyberspace*, 177.

immediately raise the passions of seasoned military leaders who see it as a threat to service (and self) identity. Every Airman who has studied the rise of "Strategic Airpower" in the US military is well aware of the rancorous and partisan debates that preceded the separation of the Army Air Corps from the Army. This paper avoids such philosophical questions and instead examines the processes and motivations behind major military organizational changes in order to determine if and how a separate Cyber Force lobby could evolve.

The historical evidence suggests that an abrupt rupturing of the organizational status quo is unlikely to occur. The evolution of organizational structures will generally be incremental. Advocates of new capabilities will push for control of the power mechanisms that foster increased autonomy. The primary mechanisms sought will be command of forces, budgeting and acquisition authority, and cognitive freedom to develop doctrine, tactics, etc. Converted leaders will be the first advocates for these power mechanisms.[165] The cycle of incremental change will continue until one or both of two conditions arise. One, organic leaders rise up in the new capability sub-community and reach peer status with the Service Chiefs and COCOM Commanders giving them the power and influence necessary to effect radical change. Two, a significant event such as great success or great failure in war occurs and provides the impetus for internal and/or external actors to force through radical change.

Conditions that favor radical change will be backed by actor motivation to lobby for such change. Internal actor motivation for change is affected by fulfillment or frustration of personal ambitions. Motivation for a separate Cyber Force is minimized if cyberspace personnel are able

---

[165] Converted leaders are those whose early careers were in another field of expertise (armor, fighters, etc.) but upon reaching senior leadership positions were placed in charge of organizations specializing in capabilities foreign to their formative experiences. In essence, these leaders are late adopters who grow to appreciate the new capability but are too late in their careers to develop a deep understanding of the full potential of it.

to rise through the service ranks, garner a respectable share of resources, and maintain doctrinal flexibility within the current organizational construct. The SOCOM example suggests that a Functional Combatant Command, when enabled with service-like authorities, can satisfy aspirations of service members who identify with their functional skill set. At present, CYBERCOM is a sub-unified COCOM and lacks the authorities of SOCOM. There is active discussion of elevating CYBERCOM to full COCOM status. If this occurs and includes authorities similar to SOCOM, it is likely internal actor motivation to seek a separate Cyber Force will be minimized. On the other hand, external actor motivation for change is influenced by the effectiveness of the organization in question. War fighting effectiveness and capable leadership that allow the US to reach full potential in the cyberspace domain are key factors in whether external actors will be motivated to consider establishing a separate Cyber Force. If under the current construct (or current plus modifications) cyberspace competencies are maximized, then creating a separate force makes no sense and will be a waste of money and effort. If, however, cyberspace competencies are not maximized under the current construct, then a separate Cyber Force will have merit. The young age of the cyber force structure means that the current organizational paradigm is in essence untested. Based on this fact, it seems unlikely external actors will develop motivation to establish a separate Cyber Force in the near term. Finally, due to the short existence of the current cyber force structure, it will be useful to reexamine the topics discussed in this monograph every five to ten years to determine changes in the environment that may contribute to advocacy for or against a separate Cyber Force.

APPENDIX A: NETWORKING AND INTERNET HISTORY

The simplest network consists of communications between two people (or machines). Two strangers who pass unnoticed in a large city do not form a network. It is necessary for them to communicate (whether verbally, physically or optically) to become a network. When they do stop and talk, exchange head-nods, or perhaps glances, then they have communicated and established a network on the most basic level in which data, information or instructions can be passed between them. From this most basic case, the form and tools of networking between humans (and later machine surrogates) grows in complexity with scientific developments and the number of persons involved. Couriers on horseback are elements of ancient networks. Later, the printed press provided mass availability of information to transmit on networks. Ship, then airborne, mail expanded the range and speed of networks. The invention of the telegraph, radio, and telephone provided the ability to code human communication into electronic or electromagnetic representations, transmit them near the speed of light, and decode them on the other end. The programmable microprocessor digitized and automated the connection and increased the speed, volume, and variety of format of information passed on the network (they also allow the control of electro-mechanical interfaces which put physical structures at risk in cyberspace).[166] Finally, satellites and the fiber optic cable boom reduced barriers to network access across the globe. The result is cyberspace, an amalgamation of interdependent networks, all built by man to facilitate communications.

Computer networking has been a major contributor to the rise of the information age. In this age, class structure is based on access to information and control of decision making versus

[166]Bell Labs created the modem to convert digital signals to electrical signals and back in 1958.

land and property ownership.[167] The eclipse of manufacturing as a percentage of US GDP evidences the impact of the information age on contemporary society.[168] The nearly unlimited ability to structure, facilitate, and augment the exchange of information through use of computers was the impetus for networking them together.[169] The technology that allowed inter-computer communication was the development of a low cost digital data transmission protocol called "packet switching".[170] In 1969 the first successful computer network message was sent over the Internet's predecessor, called ARPANET, (packet radio and packet satellite nets were also under development) and from there computer networking flourished.[171] By the late 1970's, computer networks were accessible by tens of organizations and thousands of people, but largely limited to defense and academic circles.[172] In the 1980s, commercial networks flourished and the Internet (a network of networks) came into being. Then, Sir Tim Berners-Lee took the idea of hypertext and applied it to the transfer control protocol (TCP) and domain naming system (DNS) that already underpinned the Internet to create the World Wide Web. Introduction of the first web browser followed in 1991 making the Internet functional for the common person.[173] By 1995, there were

---

[167]Hiltz and Turoff, *The Network Nation: Human Communication Via Computer*, 15.

[168]Excluding government, in 2011 services related industries accounted for $16.5 trillion of GDP while goods- producing industries accounted for $7.35 trillion. From http://www.bea.gov/iTable/ iTable.cfm?ReqID=5&step=1

[169]Hiltz and Turoff, *The Network Nation: Human Communication Via Computer*, 18**.**

[170]Ibid,13. Packet Switching is a system that divides communications into tiny pieces and uses distributed network nodes to pass the pieces around. (Internet Hall of Fame Blog)

[171]Vinton G. Cerf, Barry M. Leiner, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, and Stephen Wolff, "Brief History of the Internet" (Internet Hall of Fame), http://www.internethalloffame.org/brief-history-internet (accessed 2 February 2013).

[172]Hiltz and Turoff, *The Network Nation: Human Communication Via Computer*, xxv.

over 50,000 networks active on all seven continents and in space.[174] By June 2012 there were more than 2.4 billion Internet users equating to a 34% total penetration of world population.[175] Jane's Defense makes the illuminating point that control of the Internet may shift away from the US and Europe as user rates rise elsewhere in the world.[176]

In the US, dependence on cyberspace is pervasive in all sectors of the economy and reflected in the growth of dependence on it by the US military. As one example, Air Force aircraft derived less than 10% of their capability from installed software in the era of the F-4. This figure has increased to near 90% in the F-35.[177] In addition to the proliferation of software needed to control and operate modern weapons systems, the systems are commonly redundantly linked to the outside world via cyberspace networks. Aircraft examples of this include data links, maintenance nets, and command and control nets. The example can be repeated for weapons systems across the services and extrapolated down to devices carried by the individual soldier, sailor, airman, or marine. US weapons systems have become information platforms with kinetic

---

[173]Cade Metz, "Berners-Lee: World Finally Realizes Web Belongs to No One," *Wired.com*, June 6, 2012, http://www.wired.com/wiredenterprise/2012/06/sir-tim-berners-lee/ (accessed 23 April 2013).

[174]Vinton Cerf et al., eds., "Brief History of the Internet," *Internet Society*, October 15, 2012): 9, http://www.internetsociety.org/brief-history-internet (accessed 2 February 2013).

[175]Internet World Stats, "Worldwide Internet Users and Population Stats," *Internet World Stats.com*, June 30, 2012, http://www.internetworldstats.com/stats.htm (accessed 2 February 2013). This includes penetration only 15.6% and 27.5% in Africa and Asia respectively despite the two continents accounting for over 4 billion of the total world population.

[176]Poornima Subramaniam, Dave Clemente and Paul Twomey, "Cyber strategies and capabilities: South Asia, South East Asia and Asia-Pacific," IHS Jane's Powerpoint Briefing, September 13, 2012, slide 18, https://janes.ihs.com.lumen.cgsccarl.com/CustomPages/Janes/DisplayPage.aspx?DocType=Hybrid+Publications&ItemId=+++1519638&Pubabbrev=JIBR (accessed 20 September 2012).

[177]Maybury, "Air Force Cyber Vision 2025,"slide 9.

capabilities. This great increase in the role of cyberspace elements to the command, control and effectiveness of weapons systems has not only resulted in incredible combat effectiveness, but also introduced new avenues of vulnerability.

The Internet was developed with an open architecture and a collaborative mindset to facilitate maximum connectivity. Openness and collaboration are noble concepts, but because networks are meant to exchange information, and in the information age, information has value, the acquisition and control of it will be contested. Thus along with huge expansion of networking in the public sector provided by the Internet, exploitation and weaponization of cyberspace appeared as well. Warning of dangers in cyberspace emerged into the public sphere in 1990 with the publication of "Computers at Risk" by the National Research Council. The report warned of potential cyber threats to economic and physical infrastructures due to "bad design, imperfect implementation, weak administration, or accidents" of computer and networking systems.[178] Since 1990, waves of publications have illuminated the various nefarious activities occurring in cyberspace. Warning of a Cyber-attack "Pearl Harbor" event dates back to at least 1994 and was repeated recently by former Secretary of Defense Leon Panetta.[179]

---

[178]National Research Council Staff, *Computers at Risk: Safe Computing in the Information Age* (Washington, DC: National Academies Press, 1990), 7-8, http://site.ebrary.com.lumen.cgsccarl.com/lib/carl/ docDetail.action?docID=10056738 (accessed 3 February 2012).

[179]Elisabeth Bumiller and Thom Shanker, "Panetta Warns of Dire Threat of Cyberattack on U.S.," *The New York Times*, October 11, 2012, http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?pagewanted=all&_r=0 (accessed 6 April 2013).

APPENDIX B: REVIEW OF CYBERSPACE POLICY AND LEGISLATION

US cyberspace policy has been issued since the mid-1990s. Multiple iterations of policy documents since then have covered a variety of national and defense cyberspace topics. Presently, cyberspace policy is at the top of the list of topics receiving attention by policy makers in the Executive and Legislative branches of the US government. This was clearly exemplified when the President addressed *cybersecurity* issues in his February 2013 State of the Union address.[180] In March of this year, the Director of National Intelligence (DNI) listed cyber threats ahead of Terrorism, Transnational Crime and WMD proliferation in the intelligence community's annual threat brief to Congress. The DNI listed "Threat to US Government Supply Chains" behind the previous three, but this is also a cyberspace issue as it addresses network and computer hardware and software acquisition.[181] Cybersecurity has also been one of the four top issues listed on DoD's public website.[182] A clear sign of the focus on cyberspace issues is the fact that in the new era of declining defense budgets where keeping a steady funding line is increasingly seen as a

[180]President, Address, "State of the Union" (February 12, 2013), http://www.whitehouse.gov/state-of-the-union-2013 (accessed 6 April 2013). It should be noted that while operations in the cyberspace domain may be offensive, defensive, or exploitative, as previously discussed, the majority of literature available addresses defensive vulnerabilities of US systems under the umbrella term cybersecurity, so this term will appear much more frequently than offensive terms such as cyber-attack or cyber exploitation with regards to US policy.

[181]James R. Clapper, *Worldwide Threat Assessment of the US Intelligence Community* (Office of the Director of National Intelligence, March 12, 2013), 1-9, http://www.intelligence.senate.gov/130312/clapper.pdf (accessed 7 April 2013). The text identifies to the global supply chain in general of which cyberspace equipment producers are an element.

[182]U.S. Department of Defense, Website Header, http:/www.defense.gov (accessed 30 December 2012). The other three top issues are Afghanistan, Warrior Care and Defense Strategic Guidance.

win, cyberspace programs are winning the resource allocation competition.[183] This section reviews the most recent US national and DoD cyberspace policy documents and recent cyberspace legislation efforts.

The 2010 National Security Strategy notes that cyberspace capabilities power the daily lives of Americans and admonishes that the US must be prepared to deal with asymmetric threats which target cyberspace. One of the goals listed under "Strengthen Security and Resilience at Home" is to "Secure Cyberspace". Three lines of effort are included in this goal including: deter, prevent, detect, defend against and quickly recover from cyber intrusions and attacks, strengthen partnerships, and safeguard the Global Commons (of which cyberspace is considered a part).[184] The cyberspace objectives in the NSS are underpinned by the 2009 Comprehensive National Cybersecurity Initiative (CNCI). The major goals of the CNCI include: establish front line defense against today's immediate threats, defend against the full spectrum of threats, and strengthen the future cybersecurity environment. The CNCI includes 12 initiatives to accomplish the goals. The initiatives in the CNCI form the basis for subordinate strategies published by Executive Branch Agencies and Departments. Major lines of effort outlined in the CNCI include: provide shared network situational awareness, counterintelligence, secure the supply chain, coordinated research and development programs, define and develop deterrence strategies, and expand cyber education.[185] The US has also published the 2011 International Strategy for

---

[183]U.S. Department of Defense, *The Budget for Fiscal Year 2013*, 79, http://www.whitehouse.gov/sites/default/files/omb/budget/fy2013/assets/defense.pdf (accessed 6 April 2013).

[184]The White House, *The National Security Strategy of the United States* (May 2010), 8, 18, http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf (accessed 7 April 2013).

[185]The White House, *The Comprehensive National Cyber Security Initiative of the United States* (2009), 1-5, http://www.whitehouse.gov/cybersecurity/comprehensive-national-

Cyberspace with diplomatic, defense, and development objectives. In the international arena, the US will work to promote an open, interoperable, secure, and reliable information and communications infrastructure. The US will seek to shape the global cyberspace environment by promoting state actions guided by norms of responsible behavior, sustaining partnerships, and supporting the rule of law in cyberspace. The strategy recognizes that states are exercising national power in cyberspace, but that clearly agreed to norms of behavior are still lacking. These norms are required to prevent misunderstanding that could lead to conflict, ensure functionality of networks, and improve overall cybersecurity. The strategy dictates participation in developing international cybercrime policy as well as promoting secure technical standards. Further, the US will support civil society actors to foster freedom of expression. The US will seek a cyberspace that is open to the transfer of ideas, free from state control of content, and protective of privacy.[186] In the strategy, defense objectives will be accomplished by dissuading and deterring malicious actors. Dissuasion will be accomplished by strong network defenses able to withstand and recover from disruptions or attacks. The US will also seek global, interconnected incident detection and response capabilities. Deterrence will ensure the risk associated with attacking US cyberspace will outweigh benefits. International cooperation will be sought to investigate, apprehend and prosecute non-state malicious actors. The US will retain the right to use all necessary means, consistent with international law, to respond in self-defense to nation-state cyberspace attacks on the US or its treaty allies.[187]

---

cybersecurity-initiative (accessed 7 April 2013).

[186]The White House, *International Strategy for Cyberspace of the United States* (May 2011), 3-25, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (accessed 7 April 2013).

[187] Ibid.

The 2011 National Military Strategy (NMS) lists several goals and objectives related to cyberspace. DoD will seek the ability to fight through a degraded environment and improve the ability to attribute and defeat attacks on systems and infrastructure. Strategic Command and Cyber Command will collaborate with government and non-government entities to develop norms, capabilities, organizations, and skills. DoD will be ready to provide a broad range of options to ensure access and use of cyberspace. The Joint Force will secure the dot mil domain employing a combination of detection, deterrence, denial and multi-layered defense.[188] The NMS was supplemented in 2012 by "Sustaining Global Leadership: Priorities for 21st Century Defense" and "Defense Budget Priorities and Choices" documents. According to these documents, the US will organize forces that can conduct a combined arms campaign across all domains (including cyberspace) in order to deter and defeat aggression. The documents recognize that both state and non-state actors possess the capability to conduct espionage in cyberspace and potential to launch cyber-attacks on the US. The policy recognizes that asymmetric capabilities such as cyber warfare will be an element of anti-access, area denial challenges. Finally, DoD will work with allies and partners, and invest in advanced capabilities to defend its networks, operational capability, and resiliency in cyberspace.[189] Resources are tied to the strategy by increasing investments in defensive and offensive cyber capabilities.[190]

---

[188]US Joint Chiefs of Staff, *The National Military Strategy of the United States of America* (February 8, 2011), 8,10, http://www.jcs.mil/content/files/2011-02/020811084800_2011_NMS_-_08_FEB_2011.pdf (accessed 7 April 2013).

[189]US Department of Defense, *Sustaining Global Leadership: Priorities for 21st Century Defense* (January 2012), 3-5, http://www.defense.gov/news/defense_strategic_guidance.pdf (accessed 7 April 2013).

[190]US Department of Defense, *Defense Budget Priorities and Choices* (January 2012), 9, http://www.defense.gov/news/Defense_Budget_Priorities.pdf (accessed 7 April 2013).

The themes from the NMS are fleshed out in the 2011 DoD Strategy for Operating in Cyberspace. Threats DoD will focus on are external actors, insiders, supply chain vulnerabilities, and threats to operational ability. DoD will execute five strategic initiatives (ways) to combat these threats including: treating cyberspace as an operational domain, employing new defense operating concepts to protect networks, partnering with other government and private entities, building relationships with allies and partner nations, and leveraging an exceptional workforce and rapid technological innovations. Declaration of cyberspace as an operational domain is a "critical" organizing concept to allow DoD to organize train and equip forces in like fashion to Army, Air, and Naval Forces. New defense operating concepts include shifting operations to secure networks, practicing cyber hygiene across the Department and executing active cyber defenses to discover, detect, and mitigate threats and vulnerabilities. As a global domain with large dependency on commercial networking assets, DoD will partner and collaborate with others where it has no direct authority to mitigate risks. DoD will also seek new organizational paradigms within the total force construct to leverage expertise available in state and local governments and the private sector. In addition, DoD will seek reforms to acquisition processes that will reduce purchase cycles from seven years to less than three years and focus on spiral development rather than large systems.[191]

Although somewhat dated, the declassified 2006 National Military Strategy – Cyber Operations further delineates DoD cyberspace strategies. DoD roles in cyberspace include defense of the nation, national incident response, and critical infrastructure protection. DoD strategic priorities at the time were listed as, gain the initiative to operate within the enemy's

---

[191]US Department of Defense, *Department of Defense Strategy for Operating in Cyberspace* (July 2011), 5, http://www.defense.gov/news/d20110714cyber.pdf (accessed 7 April 2013).

OODA loop, integrate cyberspace across the range of military operations, build cyber operations capacity, and manage the cyber operations risk.[192] Included in the partially redacted text are five fundamental focus areas: network operations, kinetic actions, law enforcement, counterintelligence, and themes and messages. Six areas of focus will enable these ways including: science and technology, partnering, intelligence data and support to operations, situational awareness, law and policy, and people. These roles, strategic priorities, and ways will be accomplished by establishing eight Joint Cyberspace capabilities: battle space awareness, force generation, command and control, information operations, network-centric operations, deterrence, homeland defense, interagency integration, intergovernmental organization coordination, and non-governmental organization coordination.[193]

Several DoD Agencies have critical roles in cyberspace. Organizations such as the Defense Intelligence Agency and National Security Agency understandably do not publish comprehensive cyberspace strategies in the open domain so will not be examined here. The Defense Information Systems Agency (DISA), led by the DOD's Chief Information Officer (CIO), is a critical provider of information infrastructure for the DOD, and publishes hardware, software, and information architecture strategies relevant to the Combatant Commands and Services. DISA's Strategic Plan 2013-2018 includes focus on cyber command and control including expanding Defensive Cyber Operations and DoD Global information Grid Operations mission support. In addition, DISA will implement the Joint Information Environment (JIE)

---

[192]The OODA loop is outlined in briefings by COL John Boyd. See Frans P.B. Osinga *Science, Strategy and War: The Strategic Theory of John Boyd* (New York: Routledge, 2007) for detailed treatment on the OODA loop.

[193]US Joint Chiefs of Staff, *National Military Strategy – Cyber Operations* (2006), 3-20, http://www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/07-F-2105doc1.pdf (accessed 7 April 2013).

strategy. The JIE is a set of initiatives that will shape the future of the DoD information infrastructure. It involves moving to a single joint network architecture that will allow Cyber Command to have situational awareness of and better defend network activity.[194] Three key initiatives of the JIE include consolidating servers from across DoD organizations into three tiers of data centers, moving to cloud based computing applications, and standardizing applications.[195] Additional DISA Strategy documents that will guide DoD cyberspace warriors include the 2011 DoD Information Technology Enterprise Strategy and Roadmap, the 2012 DoD Cloud Computing Strategy, and the 2012 DoD Mobile Device Strategy V2.0.

As discussed previously, because cyberspace largely facilitates the transmission of information, all areas of the US government are concerned and involved to varying degrees. Executive Departments including the Department of Homeland Security (DHS), Department of State (DOS), Director of National Intelligence (DNI), and the Department of Justice (DOJ) have significant roles and responsibilities in cyberspace. Accordingly, there is a large body of strategy documents reflecting those roles and responsibilities, which are mentioned but not reviewed here do to scope. DoD individuals involved in cyberspace operations who interact with other government agencies will find relevant cyberspace strategy information in the following non-comprehensive list: the 2010 Quadrennial Homeland Security Review, the 2011 DHS Blueprint for a Secure Cyber Future, the 2009 National Infrastructure Protection Plan (which assigns DoD responsibility for the Defense Industrial Base (DIB), the 2010 Quadrennial Diplomacy and

---

[194]Cheryl Pellerin, "DOD Develops Cybersecurity Rules of Engagement," *American Forces Press Service*, March 20, 2012. http://www.defense.gov/News/NewsArticle.aspx?ID=67625 (accessed 14 January 2013).

[195]Defense Information Systems Agency, *DISA Strategic Plan 2013-2018*, http://www.disa.mil/About/~/media/Files/DISA/About/Strategic-Plan.pdf (accessed 6 April 2013).

Development Review, the 2009 National Intelligence Strategy, the 2009 National Counterintelligence Strategy, and the Department of Justice Strategic Plan. Other whole of government strategies that are relevant to cyberspace operations include the 2011 National Strategy for Trusted Identities in Cyberspace and the 2012 National Strategy for Global Supply Chain Security. The Department of Energy and the Department of Treasury are also significant stakeholders and address cyberspace issues to some degree in strategy documents.

While cyberspace policy abounds, Congress has been less successful in efforts to produce cyberspace legislation. Two cybersecurity bills were introduced but failed to pass Congress in the last two years. The legislative front is a contentious one based on the fact much of the activity in cyberspace is conducted by private entities on commercial infrastructure. Defense of public cyberspace issues date back to the 1980s when the breakup of AT&T combined with the 1986 Computer Security Act eliminated direct government mechanisms for assuring security of the diverse US information infrastructure.[196] Deliberate weakness was built into the 1986 bill which hamstrung the US government regarding regulating cybersecurity in the commercial sector. During the 1990s, the Clinton Whitehouse promoted policies fostering wide availability of the information infrastructure with little regard to implementing security provisions, while on the other hand acknowledging the threats posed to it via many of the studies and policy documents released during that period. By the mid-1990s, recognition of cyberspace vulnerabilities reached the level of importance to attract Executive and Congressional attention. A RAND Corporation study, a National Defense Panel study for Congress, and a Government Accountability Office (GAO) report all addressed the cybersecurity issue, which the news media then took up. At the same time, warnings emerged in books by several authors including well known futurists, the

[196]Rattray, *Strategic Warfare in Cyberspace*, 314.

Tofflers. As for policy, cyberspace vulnerabilities were listed a risk to national security in the 1996 National Security Strategy. [197] The GAO identified government information security as a high-risk area in 1997, and in 2003 expanded it to include vulnerabilities of critical infrastructures.[198]

Gregory Rattray warned in 2001 that concerns regarding diminished economic opportunities and civil liberties would severely constrain the ability of political authorities within societies like the US to take strong steps to establish cyberspace defenses.[199] The legislative issue remains in very much the same state more than a decade later, evidenced by the failure of the 2012 Cybersecurity Bill (SCB). The proposed 2012 SCB initially included mandatory security standards for businesses involved with critical cyber infrastructure. Business groups lobbied against this regulatory measure and many public interest groups joined them over individual privacy concerns. Even after the security standards were made voluntary, resistance persisted and the bill was killed.[200] While Congress may recognize the need to act and American business may want some government help on cybersecurity, efforts in the legislative arena have thus far failed. President Obama has weighed in to push the issue forward, using Executive Order to enact the measures of the failed cyber bill, but the executive order does not carry the legal weight of

---

[197]Ibid 330.

[198]Gregory C. Wilhusen, *Cybersecurity: Threats Impacting the Nation* (U.S. Government Accountability Office, April 24, 2012): 1, http://www.gao.gov/assets/ 600/590367.pdf (accessed 30 December 2012).

[199]Rattray, *Strategic Warfare in Cyberspace*, 219.

[200]Bob Krenek, "Cyber Security Act of 2012 Dies as An Executive Order is Born," *Experian Data Breach Resolution* (January 8, 2013), http://www.lexology.com/library/detail.aspx?g=15962597-dc41-4929-ad75-482a1ceaeaf4 (accessed 6 April 2013).

legislation. To emphasize this point, General Alexander in March 2013 Senate testimony urged lawmakers to move forward on cyber legislation.[201]

[201]Senate Committee, "Oversight: U.S. Strategic Command and U.S. Cyber Command."

APPENDIX C: INTERNATIONAL EFFORTS TO ESTABLISH CYBERSPACE NORMS

The attempts of the international community to establish norms in cyberspace go back to the 1990s according to Tim Maurer who conducted an examination of such policy initiatives at the UN for Harvard's Kennedy School in 2011.[202] He traces two basic threads being pursued in diplomatic and bureaucratic arms of the UN: norms for politico-military issues or cyber warfare, and norms for economic issues or cybercrime. These threads serve as a useful framework to examine work on the development of cyberspace norms.

The transnational, borderless nature of the Internet is the impetus for nations' to seek normative behaviors in cyberspace.[203] In the diplomatic arena, the Russian government's proposal of a cyberspace arms control resolution, introduced in 1998 and every year thereafter, initiated attempts to build international norms. Early resolution proposals were rejected by the US. Editorials suggested the US was opposed to the initiative because it was viewed as a way to constrain or reduce the perceived US advantage in cyber operations, because the initiative was focused on restricting free speech, and/or because Russia/China could circumvent the treaty by use of third parties (e.g. the aforementioned citizen hackers).[204] The Russian proposal started to gain wider acceptance in 2006, and in 2010 the US reversed stance and co-sponsored the latest version of the draft resolution.

---

[202]Tim Maurer, "Cyber Norm Emergence at the United Nations: An Analysis of the Activities at the UN Regarding Cyber-Security" (discussion paper 2011-11, Science, Technology, and Public Policy Program, Belfer Center for Science and International Affairs, Harvard Kennedy School, September 2011), 17, http://belfercenter.ksg.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf (accessed 18 March 2013).

[203]Ibid, 10.

[204]Ibid, 18.

Bureaucratic elements of the UN are also pursuing establishment of norms in cyberspace. An important factor in this space is the International Telecommunication Union (ITU). The ITU is charged with "building confidence and security in the use of information & communications technology," and backs two forums, the Global Cyber Agenda (GCA) and the International Multilateral Partnership Against Cyber Threats (IMPACT). The GCA engages international stakeholders to advance establishment of cyberspace norms based on five lines of effort: legal measures, technical and procedural measures, organizational structures, capacity building, and international cooperation.[205] IMPACT is the cybersecurity execution arm of ITU and provides expertise, facilities and resources for member states (193) to address cyber threats.[206] Maurer concludes that developments like these indicate norm emergence is taking place within the UN.[207]

Two significant norm building initiatives outside the UN also illuminate recent work to establish international politico-military and economic norms. These initiatives are the Tallinn Manual, which addresses issues of war and international law, and the Budapest Convention on Cybercrime. The Tallinn Manual is a NATO Cooperative Cyber Defense Center of Excellence publication released in 2013 examining how international law applies to cyberspace and warfare in particular. The manual is the result of a three-year study by an international group of experts and consists of rules and commentary reflecting international law in the cyberspace context. The

---

[205]International Telecom Union, "Global Cybersecurity Agenda," brochure, 12, http://www.itu.int/osg/csd/cybersecurity/gca/new-gca-brochure.pdf (accessed 6 April 2012)

[206]International Multilateral Partnership Against Cybercrime, "IMPACT Mission and Vision," under "About Us," http://www.impact-alliance.org/aboutus/mission-&-vision.html (6 April 2013).

[207]Maurer, "Cyber Norm Emergence at the United Nations: An Analysis of the Activities at the UN Regarding Cyber-Security," 24.

manual rejects "cyberspace as a distinct domain subject to a discrete body of law," the implication being International Law can be applied to cyberspace by identifying and applying relevant legal principles.[208] The manual examines legal concepts of warfare including use of force, armed attack, right of self-defense, etc. The manual does not in itself establish norms but provides a body of work that may serve as a basis for international legal norms in cyberspace which contribute to stability and resolution of conflicts. The Budapest Convention on Cybercrime, completed in 2001, was produced by the Council of Europe in an effort to pursue a common criminal policy aimed at the protection of society against cybercrime.[209] The convention contains articles that describe categories of cybercrime, prescribe legislative measures adopting states will use to investigate and prosecute the crimes, and rules for international cooperation and mutual assistance.[210] Twenty eight countries had ratified the convention and 100 countries use it as a guideline, reference standard, or model law as of 2010.[211] Russia failed to ratify the Budapest Convention on Cybercrime due to the document condoning cross-border searches by foreign law enforcement agencies. Ongoing debate centers on whether the Budapest Convention should be adopted as a global convention.[212] The UN Economic and Social Council produced the position

---

[208]Michael N. Schmitt, "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed," *Harvard International Law Journal Online* 13 (2012): 5, http://www.harvardilj.org/2012/12/online-articles-online_54_schmitt/ (accessed 19 April 2013).

[209] Council of Europe, "Convention on Cybercrime," (Budapest, September 23, 2001): preamble, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (accessed 6 April 2013).

[210] Ibid.

[211]Octopus Interface 2010-Workshop Brief, "The Budapest Convention on Cybercrime as a global framework: Introduction to panel discussions," Power Point briefing, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy-activity-interface-2010/presentations/Ws%203/cyber_octopus_WS_3_alexander_CCC_global_frame.pdf.

[212]Maurer, "Cyber Norm Emergence at the United Nations: An Analysis of the Activities at the UN Regarding Cyber-Security," 42.

that existing UN Conventions combined with the Convention on Cybercrime as well as the 13 universal instruments against terrorism provide the framework and legal basis for dealing with economic fraud and identity-related crime.[213] Significant actors are thus working to establish international norms for cyberspace. Commentaries on the both the Tallinn Manual and the Budapest Convention on Cybercrime suggest that there is much more work to be done.

[213]Ibid, 41.

APPENDIX D: THE ROAD TO A SEPARATE AIR FORCE

> "…the security of this country and the maintenance of world peace demand that our military establishment include a coequal component devoted exclusively to the problems of the air-to their exploration and their solution-to assurance of control of the air over our country and, if necessary, over that of an aggressor."
>
> -General Hap Arnold

The Aviation section of the Signal Corps was established in August 1907.[214] It was less than six years later in 1913 when Representative James Hay, chairman of the House Committee on Military Affairs proposed a bill that would establish a separate Air Corps as a line component of the Army. This attempt was too early in the development of airpower and was opposed by nearly all those who testified, from young fliers to the Assistant Secretary of War, in hearings on the topic.[215] Another legislative attempt occurred in 1916 by Representative Charles Lieb of Indiana who introduced a series of bills to create an autonomous Department of Aviation. The debate during this attempt was between ground officers who viewed the airplane as extension of traditional communication and observation means and air officers who were focused on the potentialities of airpower.[216] The generals that weighed in did not see a role for airpower other than to augment and support ground forces. The generals' rank and influence won out and several were even incensed by the brashness of the aviators to the point Secretary of War Newton Baker launched an investigation into their behavior.[217]

---

[214] Thomas H. Greer, *The Development of Air Doctrine in the Army Air Arm, 1917-41*, (Maxwell Air Force Base: USAF Historical Division, Research Studies Institute, Air University, 1955), 1.

[215]Ibid, 1-2.

[216]Ibid, 2-3.

[217]Ibid, 2.

The outbreak of WWI brought the first major test of US airpower. Colonel Billy Mitchell served as General Pershing's Chief of the Air Service, First Army, during the war.[218] His experiences there led to concepts for employing airpower that would underpin his post war crusade for a separate Air Force. These lessons included the principles of concentration of force, priority of counter-air action (air superiority), and centralized control of air forces by an air commander.[219] Mitchell was the bright and brash advocate for airpower after WWI, whose vociferous methods were not well received by Army leadership. General Hap Arnold would later comment that General Mitchell's doctrine was basically sound but his tactics were not very shrewd.[220] Mitchell's attempt to end around the Army Generals who stood in the way of his separate Air Force vision would end poorly.

The initial post war attempt to establish a separate air force occurred in summer 1919 when Representative Charles F. Curry introduced a bill to establish a Department of Aeronautics. The bill envisioned a single organization that would sweep in all military aviation from the Army and Navy as well as control postal aviation and aircraft development and procurement. Greer describes the negotiations for this bill as "an all-out struggle for independence by leading officers of the air arm."[221] As part of the debates, Secretary of War Newton Baker directed Assistant Secretary of War Benedict Crowell to study aviation problems and how Allied powers had dealt with them in WWI. The Crowell Group recommended a centralized Air Service under a Secretary for Air. Secretary Baker released the study, publicly opposed the findings of it, and promptly

---

[218]Alfred Hurley, *Billy Mitchell Crusader for Air Power*, 2nd ed. (Bloomington: Indiana University Press, 1975), 34.

[219]Greer, *The Development of Air Doctrine in the Army Air Arm, 1917-41,* 5.

[220] Ibid, 17.

[221]Ibid, 20.

established another board to examine the advisability of a separate department of aeronautics composed of non-flying Major General Menoher, Director of the Air Service, and four artillery officers. The Menoher Board counseled against an independent air arm on the basis that air action could not prove decisive against ground forces and would violate the principle of unity of command. Secretary Baker apparently preferred this report as he stamped his approval and forwarded it to the Senate Committee on Military Affairs.[222] This incident of a policy maker unhappy with a commission report orchestrating another investigation was repeated in subsequent years. At the same time, General Pershing additionally enlisted a study of lessons from WWI, known as the Dickman Board. This Board concluded that "nothing in the war indicated that air activities could be conducted independently of ground troops so as to affect materially the outcome of the struggle."[223] This lent to the General's view and advice to Secretary Baker that a separate air arm was inadvisable. Secretary of the Navy Josephus Daniels and Assistant Secretary Franklin D. Roosevelt were also hostile to the idea of a separate air arm. Some in the Navy publicly declared in an unsigned position paper that those advocating for a separate air arm were either naïve or rank hungry opportunists.[224] The result of this go around was the formal designation of the Air Service within the Army as a combatant arm. However, it did not alter any command relationships that existed.

The debates, reports and legislation efforts surrounding a separate air arm continued in the 1920s, meeting similar resistance. Brigadier General Mitchell conducted a public crusade during this period, while at the same time more moderate air leaders looked for ways to maximize

---

[222] Ibid, 20-21.

[223] Ibid, 24.

[224]Ibid, 24-25.

airpower offensive capabilities within the current construct. Arguably the most successful and temperate of these others was Major General Mason Patrick who served as Chief of the Air Service, AEF, in WWI and Chief of the Air Service from 1921-1927. A Pershing classmate and Corps of Engineering officer, Patrick embraced his role as Air Service leader, gaining both his flight certificate and currency in airpower doctrine developments.[225] Rather than a separate force, Patrick lobbied for the power levers behind an effectively separate air arm and did so in terms his fellow line officers could relate too. He primarily sought the ability to shape the size and type of aircraft acquisitions, the independent budgeting authority to control that process, and the command authority for centralized control of air forces necessary to concentrate force effectively. He made logical airpower employment arguments in the subtext of a war fought by all combat arms branches vice arguing that airpower could outright win a conflict. In addition, he framed the organization he envisioned as similar to the Marine Corps' relation to the Navy, which likely made his initiatives more palatable and harder to refute outright.[226]

The backdrop to Major General Patrick's initiatives was a wide open and divided debate in the civilian institutions that made policy and law. In 1924 the House Military and Naval Affairs committees commissioned a study on the question, known as the Lampert Commission. The Lampert Commission recommended a unified independent air force, tasked to support the Army and Navy as required, assistant secretaries for air in the War, Navy and Commerce departments, and a Department of National Defense to coordinate the armed forces' efforts.[227] While the Lampert Commission was underway, the Secretaries of War and Navy requested

---

[225]Hurley, *Billy Mitchell Crusader for Air Power*, 33.

[226]Greer, *The Development of Air Doctrine in the Army Air Arm, 1917-41,* 26-27.

[227] Ibid, 26-27.

President Coolidge launch a separate study. That group was known as the Morrow Board. After conducting research, the board released findings counter to the Lampert Commission including advising against a separate department of air and against a Department of Defense. Further, the Morrow Board released their report two weeks before the Lampert Commission in November 1925 and drew the lion's share of attention to their findings as a result. At the same time, Brigadier General Billy Mitchell was waging a public relations campaign to forward strategic bombing theories and lobby for a separate Air Force. Unfortunately, to draw attention, Mitchell increasingly used inflammatory claims that he could not fully prove and which drew the ire of Secretary of War Weeks as well as drawing the displeasure of President Coolidge. Mitchell's clashes with leadership resulted in a loss of his position, return to the grade of Colonel, and transfer out of Washington DC to Texas. In Texas, he continued to press for change. The language in his press releases moved toward accusing superiors of negligence and of possibly intimidating congressional witnesses. Mitchell was eventually brought before courts martial in late 1926, found guilty of conduct prejudicial to good order and discipline, and effectively forced to resign. In his biography on Mitchell, Alfred Hurley speculated that Mitchell's court martial was a necessary cathartic event that served to focus Presidential Coolidge's Administration on many of the Airpower advocates' issues.[228] The rancorous debate continued until Congress passed the Air Corps Act in July 1926. The act created an Assistant Secretary of War responsible for air matters, an air section in each division of the General Staff, command of flying units by rated officers, and a five-year Air Corps equipment and personnel expansion program. While the debates in the 1920s brought some changes, the political and economic climate at the time was not conducive to radical changes in the military organizational structure. The Air Corps Act

[228]Hurley, *Billy Mitchell Crusader for Air Power,* 104-109.

would quiet the debate for nearly a decade and the War Department generals and Navy admirals were seen as the victors in this round.[229]

Debate resumed in the 1930s and incremental progress towards independence was achieved based on recommendations of two inquiries known as the Drum and Baker boards. The result of recommendations was the establishment of GHQ Air Force, giving an airman operational control of air units. Prior to this, Air Corps units had been under the command of Army Corps area commanders. The Chief of the Air Corps continued to be responsible for acquisition, personnel, training, and doctrine.[230] Under this structure, the Chief of Staff of the Air Corps and the GHQ commander reported separately, but equally, to the War Department.[231] The organizational change was important in that it put control of Airpower capabilities under an airman, but it remained an incremental organizational change and had serious flaws. Perhaps the most significant flaw was the fact control of the means (equipping) was in different leadership hands than control of the ways (training).

Foreshadows of World War II prompted President Franklin Roosevelt to conduct a huge buildup of the military and provided impetus for the next significant organizational change, but would put outright independence on hold.[232] The Army Air Forces (AAF) were established on June 20, 1941. General Hap Arnold became the single commander for air, over the Chief of the

---

[229]The court martial of Mitchell may have had a significant quieting effect on airpower advocates. While one court martial may not be significant in a modern sized military service, the Air Corps had less than 10,000 personnel in 1926, so it is likely the proceedings made a significant impression on a small aviation officer corps.

[230]Wolk, *Toward Independence, The Emergence of the US Air Force 1945-1947*, 3-4.

[231]Ibid, 4-5.

[232]Air Force strength went from 23,400 in 1939 to 51,100 in 1940 to 152,100 in 1941. (1997 Air Force Almanac)

Air Corps and a redesignated GHQ. Wartime planning efforts combined with the support of General Marshall led to the elevation of General Arnold to full membership on the US Joint Chiefs of Staff. A further reorganization ordered by General Marshall in 1942 established the AAF as coequal with Army Ground and Service Forces.[233] Herman Wolk suggested that acceptance of Hap Arnold and his staff in the highest joint planning councils was tacit acceptance of the air arm as an equal to the Navy and Army.[234]

Discussions for post war reorganization of the military occurred while the war was ongoing. Arguments about organization focused on unity of command and the minimization of inter-service parochialism. The two threads devolved from difficulties during the war getting the services to act in an integrated manner and fear of unproductive competition for resources during the expected post war draw-down. A significant report was penned by a committee commissioned by the Joint Chiefs of Staff. The committee majority recommended an independent Air Force as well as a National Department of Defense to be led by a civilian.[235] Notably the senior Navy member of the committee opposed the recommendations. Admiral Richardson opposed the Air Force idea for fear of losing the Navy's air arm. In addition, other leading admirals opposed a unified department of defense on grounds it was too large to be manageable and would diminish the influence of the Navy.[236] It is interesting to note that Army leaders, after over two decades of examination and compounding incremental changes were willing to accept an independent Air Force. Navy leaders, on the other hand, who didn't experience the same incremental changes

---

[233]Wolk, *Toward Independence, The Emergence of the US Air Force 1945-1947*, 6-7.

[234]Ibid, 7.

[235]Ibid, 10.

[236]Ibid, 12.

within their Service, remained extremely resistant to the idea even as World War II was coming to a close. Army leaders also had years of practice splitting the budget between land and air forces, another fact the Navy was not subject too since it had independent budgeting mechanisms through the Department of the Navy.

General Hap Arnold played a pivotal role in the interwar and post war debates. Two key factors contributed to the effectiveness of his advocacy for a separate Air Force. The first factor was his position and wartime performance on the Joint Chiefs of Staff. He not only had a peer-level seat at the highest military tables, he also had credibility with the leaders who had the power levers necessary to shape the post-war military organizational structure. Second, Gen Arnold could use wartime Airpower experiences as vignettes to support his arguments. He could leverage events such as the surrender of Japan after the nuclear bombings to illustrate the strategic impact of airpower. In addition, he could leverage the strategic planning his staff, essentially co-equal to their Army and Navy counterparts, were able to accomplish after the 1942 reorganization.[237] Demonstrated wartime successes carried far more weight than prewar hypotheticals in the ongoing debate for a separate Air Force.

The post war debate pitted nearly all sides against Navy resistance. The Air Force idea had powerful advocates in the evolved debate. General Eisenhower was a convert to both the ideas of a separate Air Force and a unified Department of Defense arguing in their favor before the Senate. President Truman favored the ideas as well and strongly advocated for a unified department of defense in which an Air Force would be an equal to the Navy and Army. The Navy civil and military leaders continued to work in opposition to both ideas for fear the Army would subsume the Marines, the Air Force would walk away with naval aircraft, and a Defense

[237]Ibid, 13.

Secretary with appropriate power could intervene in their budgeting process; all significantly diminishing Navy power.[238] Despite being charged by the President to resolve remaining issues, Secretary of War Patterson and Secretary of the Navy Forrestal could not work out differences on the post war defense structure. President Truman grew frustrated and ordered them to draft the legislation, dictating that it would include three military departments and a Department of National Defense headed by a civilian secretary. They went back to work to comply with the President's direction and the final result was the National Security Act of 1947 which created a separate Air Force (and Department of Defense) after decades of study, debate, and politicking.

[238]Ibid, 18.

APPENDIX E: CYBERSPACE RESPONSIBILITIES IN THE US GOVERNMENT

Cyberspace responsibilities are spread across the government and significant players reside outside of the Department of Defense. The Department of Homeland Security (DHS) has been assigned the responsibility to act as the coordinator for the overall national cyber security effort. In addition, DHS will defend civil executive branch information and communication systems (.gov domain), coordinate defense of privately owned and operated elements of the US Critical Infrastructure, and assist subordinate governments (state, local, tribal) to secure their information systems.[239] Within the Department of Justice, the FBI has responsibility to investigate cyber-based terrorism, espionage, hacking, and fraud.[240] The Department of Energy and the Secret Service also have some degree of responsibility for defending the nation in cyberspace.[241] The fact that cyberspace responsibilities are spread across government agencies means significant coordination between these organizations and the DoD will be vital for the execution of an effective defense of the US in cyberspace.

The DoD is responsible for fighting the nation's wars and defending the country. The borderless, largely civilian characteristic of cyberspace in the US complicates the defense task, which is facilitated by many agencies outside the DoD as noted above. General Alexander in recent testimony indicated, however, that if entities within the US were attacked in cyberspace,

---

[239]US Department of Homeland Security, *Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the the Homeland Security Enterprise* (November 2011). Also, see DHS' June 2011 *Preventing and Defending Against Cyber Attacks* for a summary of DHS strategies, plans, cyber centers, program initiatives, partnerships, exercises, and workforce development efforts in cyberspace.

[240]The Federal Bureau of Investigation, "Cyber Crime," FBI, http://www.fbi.gov/about-us/investigate/cyber (accessed 9 April 2013).

[241]DOE executes cybersecurity programs to secure the energy infrastructure. The Secret Service investigates financial cybercrimes such as credit card data theft.

"then Cybercom would step in."[242] DoD also has the responsibility for protecting military networks (.mil).

The Office of the Secretary of Defense (OSD) has responsibility for direction, policy and oversight of military forces and several OSD elements have a major role in cyberspace. The Assistant Secretary of Defense for Global Strategic Affairs (GSA) is responsible for overall DoD Cyberspace strategy and policy and works for the Under Secretary of Defense (USD) for Policy. The USD for Policy co-chairs the Cyber Integration Group, a governance mechanism that assigns actions across DoD to accomplish the Defense Strategy for Operating in Cyberspace.[243] The Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer is responsible for ensuring DoD information and information technologies are available and dependable.[244] DoD Agencies also have responsibilities in cyberspace. The Defense Advanced Research Projects Agency is responsible for conducting research in order to create and prevent strategic surprise.[245] The Defense Information Systems Agency provides, operates, and assures information capabilities and the global enterprise information infrastructure.[246] The

---

[242]Cheryl Pellerin, "Cybersecurity Involves Federal, Industry Partners, Allies," *American Forces Press Service*, November 8, 2012, http://www.defense.gov/news/newsarticle.aspx?id=118479 (accessed 30 December 12). *Washington Post* articles support the reality of this position, see Ellen Nakashima stories from 9 Aug and 14 Nov 2012 discussing DoD authorizations to act outside military networks and a new secret Presidential directive (PPD20) giving authorization and clearing the way for finalizing new ROE.

[243]House Armed Services Committee, *ASD Creedon Testimony HASC on Emerging Threats and Capabilities* (March 20, 2012), 3-4, http://armedservices.house.gov/index.cfm/files/serve?File_id=d2585a85-6fca-42d7-b8aa-be1e7e8496e2 (accessed 9 April 2013).

[244]House Committee, *Statement by Teresa M. Takai*, 2.

[245]US Defense Advanced Research Projects Agency, "Our Work," DARPA, http://www.darpa.mil/our_work/ (accessed 9 April 2013).

National Security Agency/Central Security Service protects national security systems and produces foreign signals intelligence information.[247]

[246]US Defense Information Systems Agency, "Our Mission," DISA, http://disa.mil (accessed 9 April 2013).

[247]National Security Agency Central Security Service, "Our Mission," NSA/CSS, http://www.nsa.gov (accessed 9 April 2013).

APPENDIX F: SERVICE COMPONENT CYBER ORGANIZATIONS

Major General Suzanne Vautrinot currently leads the Air Force Cyber Component and is dual hatted as both the 24th Air Force (24 AF) Commander and the Air Force Cyber Command (AFCYBER) Commander. 24 AF/AFCYBER has three roles including providing forces to USCYBERCOM, to operate and defend the Air Force Portion of the DoD network, and to organize, train, and equip USAF cyber personnel. Subordinate cyber elements include the 67th Network Warfare Wing, the 624th Operations Center, the 688th Information Operations Wing, and the 689th Combat Communications Wing. The organization consists of 17,000 total force personnel and contractors executing full spectrum cyber operations.[248]

Lieutenant General Rhett Hernandez currently leads the Army Cyber Component. He is dual hatted as the 2nd Army Commander and the Army Cyber Command (ARCYBER) Commander. ARCYBER/2nd Army is responsible for network operations and defense of all Army networks, and conducts cyberspace operations in support of Full Spectrum Operations. Subordinate cyber elements include the 9th Signal Command and the 1st Information Operations Command.[249] The organization consists of more than 21,000 Army Soldiers, civilians, and contractors worldwide.[250]

Vice Admiral Michael Rogers currently lead the Navy cyber component. He is dual hatted as the 10th Fleet Commander and the US Fleet Cyber Command Commander. The 10th Fleet mission is to execute full spectrum of cyberspace, electronic warfare, information

---

[248]House Committee, *Statement of MGEN Suzanne M. Vautrinot*, 1-12.

[249]U.S. Army Cyber Command, website, U.S. Army, http://www.arcyber.army.mil/org (accessed 23 April 2013).

[250]House Committee, *Statement by Lieutenant General Rhett Hernandez.*

operations, and signal intelligence capabilities across cyberspace, the electromagnetic spectrum, and Space domains. Fleet Cyber Command is also responsible for networks and cryptology in support of forces afloat and ashore. The command consists of 14,000 Sailors and civilians at more than twenty commands dispersed worldwide.[251]

Lieutenant General George Flynn leads the Marine cyber component known as MARFORCYBER. MARFORCYBER will plan, coordinate, integrate, synchronize and direct full spectrum Marine Corps cyberspace operations, defense and offense. Subordinate organizations include the Marine Corps Network Operations Security Center (MCNOSC); and the Marine Corps Cryptologic Support Battalion's (MCSB) Company L, which will consist of 800 personnel when filled out.[252]

[251]U.S. Fleet Cyber Command, U.S. Tenth Fleet, "U.S. Fleet Cyber Command Mission," U.S. Navy, http://www.fcc.navy.mil (accessed 9 April 2013).

[252]House Armed Services Committee, *Statement of Lieutenant General Richard P. Mills Deputy Commandant Combat Development and Integration & Commanding General, Marine Corps Combat Development Command July 25, 2012*, 2-4, http://armedservices.house.gov/index.cfm/files/serve?File_id=d5a13bad-73e9-4543-ab0b-d84e201bf844 (accessed 9 April 2013).

BIBLIOGRAPHY

Australia. Attorney General's Department. *Australian Government Cybersecurity Strategy*. 2009. http://www.ag.gov.au/cybersecurity (accessed 20 August 2012).

Bayles, William J. "The Ethics of Computer Network Attack." *Parameters* 31, no. 1 (Spring 2001): 44-58. http://search.proquest.com.lumen.cgsccarl.com/docview/198019494 (accessed 12 September 2012).

Bell, Bryan and Eric Trias. "Cyber This, Cyber That…So What?" *The WSTIAC Quarterly* 9, no. 4 (2009): 7-15. http://wstiac.alionscience.com/pdf/WQV9N4_ART02.pdf (accessed 23 August 2012).

Berg, Paul. "Air Force Cyber Command: What it Will Do and Why We Need It," *Air & Space Power Journal Espanol* (February 20, 2007). http://www.airpower.au.af.mil/ apjinternational/apj-s/2007/1tri07/bergeng.html

Birdwell, David and Robert Mills. "War Fighting in Cyberspace: Evolving Force Presentation and Command and Control." *Air & Space Power Journal* (Spring 2011):26-36. http://www.airpower.au.af.mil (accessed 10 February 2013).

Brown, Bryan D. "U.S. Special Operations Command: Meeting the Challenges of the 21st Century." *Joint Forces Quarterly* 40 (1st Quarter 2006): 38-43. http://www.ndu.edu/ press/lib/pdf/jfq-40/JFQ-40.pdf (accessed 24 April 2013).

Buennemeyer, Timothy K. "A Strategic Approach to Network Defense: Framing the Cloud." *Parameters* 41, no. 3 (Autumn 2011): 43-58. http://search.proquest.com.lumen. cgsccarl.com/docview/ 928971316 (accessed 23 August 2012).

Builder, Carl H. *The Masks of War: American Military Styles in Strategy and Analysis.* Baltimore: The Johns Hopkins University Press, 1989.

Cairns-McFeeters, Gina. "United States Cyber Command." *The CIP Report* 9, no. 7 (January 2011): 5-6, 20. http://cip.gmu.edu/archive/CIPHS_TheCIPReport_January2011_ Cybersecurity.pdf (accessed 23 August 2012).

Carr, Jeffrey. *Inside Cyber Warfare.* 2nd ed. Sebastopol: O'Reilly Media, 2012.

Cerf, Vinton G., Barry M. Leiner, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daneil C. Lynch, Jon Postel, Larry G. Roberts, and Stephen Wolff. "Brief History of the Internet." Internet Hall of Fame. http://www.internethalloffame.org/brief-history-internet (accessed Feb 2, 2013).

Cetron, Marvin J., Owen Davies, Stephen F. Steele, and Cynthia E. Ayers. "World War 3.0: Ten Critical Trends for Cybersecurity." *The Futurist* 43, no. 5 (Sep/Oct 2009): 40-49. http://search.proquest.com.lumen.cgsccarl.com/docview/218565971/fulltextPDF? accountid=28992 (accessed 12 September 2012).

Choucri, Nazli, Jeremy Ferdwa, and Stuart Madnick. “Institutional Foundations for Cyber Security: Current Responses and New Challenges.” Working Paper CISL# 2009-03, Massachusetts Institute of Technology, 2010. http://web.mit.edu/smadnick/www/wp/2010-03.pdf (accessed 24 April 2013).

Clapper, James R. *Worldwide Threat Assessment of the US Intelligence Community*. Office of the Director of National Intelligence, March 12, 2013. http://www.intelligence.senate.gov/130312/clapper.pdf (accessed 7 April 2013).

Clarke, Richard and Robert Knake. *Cyber War: The Next Threat to National Security and What to Do About It.* New York: HarperCollins, 2010.

Cloud, Donald Wayne. “Integrated Cyber Defenses: Towards Cyber Defense Doctrine.” Master’s thesis, Naval Postgraduate School, December 2007. https://www.hsdl.org/?view&did=482961 (accessed 19 January 2013).

Cullather, Nick. “Bombing at the Speed of Thought: Intelligence in the Coming Age of Cyberwar.” *Intelligence & National Security* 18, no. 4 (Winter 2003): 141-154. http://fw8pk7vf4q.search. serialssolutions.com/ ?ctx_ver=Z39.88-2004&ctx_enc=info%3Aofi%2Fenc%3AUTF-8&rfr_id=info:sid/summon.serialssolutions.com&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rft.genre=article&rft.atitle=Bombing+at+the+Speed+of+Thought%3A+Intelligence+in+the+Coming+Age+of+Cyberwar&rft.jtitle=Intelligence+and+National+Security&rft.au=Cullather%2C+Nick&rft.date=2003-12-01&rft.issn=0268-4527&rft.volume=18&rft.issue=4&rft.spage=141&rft.epage=154&rft_id=info:doi/10.1080%2F02684520310001688907&rft.externalDBID=n%2Fa&rft.externalDocID=10_1080_02684520310001688907 (accessed 12 September 2012).

Crosston, Matthew. "Virtual Patriots and a New American Cyber Strategy: Changing the Zero-Sum Game." *Strategic Studies Quarterly* 6, no. 4 (Winter 2012): 100-117.

Dillon, Connie. "AFSCP commander speaks at 11th Annual Air Force IT Day event." Air Force Space Command Public Affairs. http://www.af.mil/news/story.asp?storyID=123322006. (accessed 4 January 2013).

Donley, Michael B. “Remarks of the Honorable Michael B. Donley Secretary of the Air Force Credit Suisse/McAleese Aerospace and Defense Investor Conference - New York City, November 29, 2012.” http://www.af.mil/shared/media/document/AFD-121130-021.pdf (accessed 4 January 2013).

Elder, Bob. “Air Force Cyber Operations Command.” PowerPoint Briefing, 5 Jan 2007. http://www.powershow.com/view/d6fbe-NzA2N/Air_Force_Cyber_Operations_Command_Mission_Warfighting_powerpoint_ppt_presentation (accessed 24 April 2013).

Evans, Karen, Franklin Reeder. “A Human Capital Crisis in Cybersecurity, Technical Proficiency Matters.” Whitepaper, Center for Strategic & International Studies, 2010. http://csis.org/files/publication/100720_Lewis_HumanCapital_WEB_BlkWhteVersion.pdf (accessed 24 April 2013).

Fadok, David and Richard Raines. “Driving towards Success in the Air Force Cyber Mission,” *Air & Space Power Journal* 26, no. 5 (Sep-Oct 2012): 4-12. http://www.dtic.mil/dtic/tr/fulltext/u2/a568285.pdf (accessed 10 February 2013).

Fahrenkrug, David. “Cyberspace Defined.” http://www.au.af.mil/au/awc/awcgate/wrightstuff/cyberspace_defined_wrightstuff_17may07.htm (accessed 3 September 2012).

Farrell, John F. and Adam B. Lowther. “From the Air: Rediscovering Our Raison D’etre.” *Air & Space Power Journal* 26, no. 4 (July-August 2012): 61-102.

Farwell, James P. "Industry's Vital Role in National Cyber Security." *Strategic Studies Quarterly*, 6, no. 4 (Winter 2012): 10-35.

Feickert, Andrew. “The Unified Command Plan and Combatant Commands: Background and Issues for Congress,” Congressional Research Service, July 17, 2012. http://www.fas.org/sgp/crs/natsec/R42077.pdf (accessed 30 December 2012).

Fryer-Biggs, Zachary. “Panetta Green Lights First Cyber Operations Plan.” *Defense News*, June 6, 2012. http://www.defensenews.com/article/20120606/DEFREG02/306060010/Panetta-Green-Lights-First-Cyber-Operations-Plan (accessed 14 January 2013).

Gardels, Nathan. “Cyberwar: Former Intelligence Chief Says China Aims at America's Soft Underbelly.” *New Perspectives Quarterly* 27, no. 2 (Spring 2010): 15.

Greengard, Samuel. “The New Face of War.” *Communications of the ACM* 53, no. 12 (December 2010): 20-22.

Greer, Thomas H. *The Development of Air Doctrine in the Army Air Arm, 1917-1941*. Maxwell Air Force Base: USAF Historical Division, Research Studies Institute, Air University, 1955.

Gregory, Derek. “The Everywhere War.” *The Geographical Journal* 177, no. 3 (Sep 2011): 238-250. http://www.lsa.umich.edu/UMICH/eihs/Home/Events/gregory_everywhere_war.pdf (accessed 24 April 2013).

Gross, Eric. “Some tech-talks in Security, Cryptography, and Privacy.” 2010 Google Faculty Summit: Security at Scale. Video of Presentation. http://research.google.com/pubs/SecurityCryptographyandPrivacy.html (accessed 14 January 2013).

Hagendoorn, Louk, Markus Prior and Paul Sniderman. “Predisposing Factors and Situational Triggers: Exclusionary Reactions to Immigrant Minorities.” *The American Political Science Review* 98, no. 1 (February 2004): 35-49. http://search.proquest.com.lumen.cgsccarl.com/docview/214413164/abstract?accountid=28992> (accessed 26 December 2012).

Hiltz, Starr Roxanne, and Murray Turoff. *The Network Nation: Human Communication Via Computer*. Rev. ed. Cambridge: Massachusetts Institute of Technology Press, 1993.

Hollis, David M. “USCYBERCOM The Need for a Combatant Command versus a Subunified Command.” *Joint Forces Quarterly* 58 (3rd Quarter, July 2010): 48-54. http://www.ndu.edu/press/jfq-58.html (accessed 24 April 2013).

Hurley, Alfred. *Billy Mitchell Crusader for Air Power*. 2nd ed. Bloomington: Indiana University Press, 1975.

Hughes, Rex. “A Treaty for Cyberspace.” *International Affairs* 86, no. 2 (March 2010): 523-541.

IHS Jane’s. “Cyber strategies and capabilities: South Asia, South East Asia and Asia-Pacific.” Powerpoint Briefing by Poornima Subramaniam, Dave Clemente and Paul Twomey, 13 September 2012. https://janes.ihs.com.lumen.cgsccarl.com/CustomPages/Janes/DisplayPage.aspx?DocType=Hybrid+Publications&ItemId=+++1519638&Pubabbrev=JIBR (accessed 20 September 2012).

Johnson, David R., David Post. “Law and Borders--The Rise of Law in Cyberspace.” *Stanford Law Review* 48, no. 5 (May 1996): 1367-1402.

Kallberg, Jan. “Designer Satellite Collisions from Covert Cyber War.” *Strategic Studies Quarterly* 6, no.4 (Spring 2012): p124-136. http://www.dtic.mil/dtic/tr/fulltext/u2/a562109.pdf (accessed 6 January 2013).

Kinne, Christopher E., USAF. “Preserving the Industrial Base.” *Air Force Journal of Logistics* 34 no. 1/2 (2010): 38-48.

Krekel, Brian. *Capability of the People’s Republic of China to Conduct Cyber Warfare and Computer Network Exploitation Prepared for The US-China Economic and Security Review Commission*. McLean: Northrop Grumman Corporation, October 9, 2009. http:// http://www.uscc.gov/ /researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdfresearchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf (accessed 19 September 2012).

Kuhn, Thomas. *The Structure of Scientific Revolutions.* 3rd ed. Chicago: The University of Chicago, 1996.

Kushner, David. “Standing guard over cyberspace.” *IEEE Spectrum* 39, no. 5 (May 2002): 68-70.

“The Law of Cyberspace.” *Harvard Law Review* 112, no. 7 (May 1999): 1574-1704.

Levin, Carl. *Opening Statement at SASC Hearing on US Strategic Command and US Cyber Command for FY 2014, Tuesday, March 12, 2013*. http://www.levin.senate.gov/newsroom/speeches/speech/opening-statement-at-sasc-hearing-on-us-strategic-command-and-us-cyber-command-for-fy-2014 (accessed 16 March 2013).

Lewis, James. *Cybersecurity Two Years Later: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency*. Washington, DC: Center for Strategic and International Studies, 2011.

Lewis, James. *Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency*. Washington, DC: Center for Strategic and International Studies, 2008.

Liang, Qiao, and Wang Xiangsui. *Unrestricted Warfare*. Beijing: PLA Literature and Arts Publishing House, February 1999. http://www.cryptome.org/cuw.htm (accessed 6 April 2013).

Libicki, Martin C. and RAND Corporation. *Conquest in Cyberspace: National Security and Information Warfare*. New York: Cambridge University Press, 2007. http://carl.summon.serialssolutions.com/document/show?id=FETCHMERGED-carl_catalog_3635251&s.q=Conquest+in+Cyberspace%3A+National+Security+and+Information+Warfare&spellcheck=true (accessed 12 September 2012).

Liff, Adam P. "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War." *Journal of Strategic Studies* 35, no. 3 (June 2012): 401-428. http://www.tandfonline.com/doi/abs/10.1080/01402390.2012.663252#preview (accessed 24 April 2013).

Lim, Tai Wei. "Implications of the People's Liberation Army's Technocratization for US Power in East Asia." *Asian Affairs, An American Review* 31, no. 1 (Spring 2004): 30-39. http://www.tandfonline.com/doi/abs/10.3200/AAFS.31.1.30-40 (accessed 24 April 2013).

Lin, Patrick, Fritz Allhoff, and Neil C. Rowe. "Computing Ethics: War 2.0: Cyberweapons and Ethics." *Association for Computing Machinery. Communications of the ACM* 55, no. 3 (Mar 2012): 24-26. http://www3.nd.edu/~mlee20/Cyberweapons_Ethics.pdf (accessed 24 April 2013).

Locher, James R., III. "Has it Worked? The Goldwater-Nichols Reorganization Act." *Naval War College Review* 54, no. 4 (Autumn 2001): 95-115. http://www.usnwc.edu/getattachment/744b0f7d-4a3f-4473-8a27-c5b444c2ea27/Has-It-Worked--The-Goldwater-Nichols-Reorganizatio (accessed 24 April 2013).

Lynn, William J. III. "Defending a New Domain: The Pentagon's Cyberstrategy." *Foreign Affairs* 89, no. 5 (September/October 2010): 97-108. http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA527707&Location=U2&doc=GetTRDoc.pdf. (accessed 24 April, 2013).Mandiant Intelligence Center Report. Webpage. http://intelreport.mandiant.com/ (accessed 18 March 2013).

Manson, George P., III. "Cyberwar: The United States and China Prepare For the Next Generation of Conflict." *Comparative Strategy* 30, no. 2 (May 2011): 121-133. http://dx.doi.org/10.1080/01495933.2011.561730 (accessed 12 September 2012).

Maurer, Tim. "Cyber Norm Emergence at the United Nations: An Analysis of the Activities at the UN Regarding Cyber-Security." Discussion Paper 2011-11, Science, Technology, and Public Policy Program, Belfer Center for Science and International Affairs, Harvard Kennedy School, September 2011. http://belfercenter. ksg.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf (accessed 18 March 2013).

Maybury, Mark T. “Air Force Cyber Vision 2025.” Powerpoint Briefing, 17 July 2012. http://www.afa.org/events/Breakfasts/MayburyPPT.pdf (accessed 30 January 2013).

McAfee Corporation. *Smarter Protection for the Smart Grid*. Santa Clara: McAfee, 2012. http://www.mcafee. com/us/resources/reports/rp-smarter-protection-smart-grid.pdf (accessed 24 April 2013).

McConnell, Mike. “Cyberwar Is the New Atomic Age.” *New Perspectives Quarterly* 26, no. 3 (Summer 2009). http://www.digitalnpq.org/archive/2009_summer/20_mcconnell.html (accessed 24 April 2013).

McGarvey, Robert. “2013’s 5 Biggest Online/Mobile Cyber Threats.” *Credit Union Times.com*, December 10, 2012. http://www.cutimes.com/2012/12/10/2013s-5-biggest-online-mobile-cyber-threats?ref=hp&t=technology&page=4 (accessed 3 January 2013).

Mesic, Richard, Myron Hura, Martin C. Libicki, Anthony M. Packard, and Lynn M. Scott. *Air Force Cyber Command (Provisional) Decision Support.* Santa Monica: RAND, 2010. http://www.rand.org (accessed 3 January 2013).

Munro, Neil. “Sketching a National Information Warfare Defense Plan.” *Communications of the ACM* 39, no. 11 (Nov 1996): 15-17.

Nakashima, Ellen. “Obama signs secret directive to help thwart cyberattacks”. *Washington Post*, November 14, 2012. http://articles.washingtonpost.com/2012-11-14/world/35505871_1_networks-cyberattacks-defense (accessed 30 December 2012).

Nakashima, Ellen. “Pentagon proposes more robust role for its cyber-specialists”. *Washington Post*, August 09, 2012. http://articles.washingtonpost.com/2012-08-09/world/35491430_1_cyber-command-military-action-networks (accessed 30 December 2012).

Nakashima, Ellen. “Pentagon to Boost Cybersecurity Force.” *Washington Post*, January 27, 2013. http://articles.washingtonpost.com/2013-01-27/world/36583575_1_cyber-protection-forces-cyber-command-cybersecurity (accessed 17 March 2013).

Naraine, Ryan. “10 security stories that shaped 2012, Guest Editorial by Costin Raiu.” *ZDNet.com*, December 10, 2012. http://www.zdnet.com/10-security-stories-that-shaped-2012_p2-7000008576/ (accessed 3 January 2013).

National Research Council of the National Academies. Committee on Deterring Cyberattacks. *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US Policy*. Washington DC: National Academies Press, 2010. http://site.ebrary.com.lumen.cgsccarl.com/lib/carl/docDetail.action?docID=10425159&p00=21st%20century%20chinese%20cyberwarfare (accessed 20 September 2012).

National Research Council Staff. *Computers at Risk: Safe Computing in the Information Age.* Washington DC: National Academies Press, 1990. http://site.ebrary.com.lumen.cgsccarl.com/lib/carl/docDetail.action?docID=10056738 (accessed 3 February 2012).

Oakley, John. “Cyber Warfare: China's Strategy to Dominate in Cyber Space.” Master’s thesis, US Army Command and General Staff College, 2011.

Octopus Interface 2010-Workshop Brief, “The Budapest Convention on Cybercrime as a global framework: Introduction to panel discussions,” Power Point briefing, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy-activity-interface-2010/presentations/Ws%203/cyber_octopus_WS_3_alexander_CCC_global_frame.pdf

Office of the Secretary of Defense. *Annual Report to Congress Military and Security Developments Involving the People’s Republic of China 2011*. Washington DC: Government Printing Office, 2011.

O'Mara, Raymond. “Clearing the Air: Airpower Theory and Contemporary Airpower.” *Air Force Journal of Logistics* 34, no. 1, 2, and Annual (2010): 52-71. http://www.aflma.hq.af.mil/shared/media/document/AFD-101122-025.pdf (accessed 24 April 2013).

Osborne, William B., Scott A. Bethel, Nolen R. Chew, Philip M. Nostrand, and YuLin G. Whitehead. “Information Operations: A New War-Fighting Capability.” Research paper presented to Air Force 2025, Air University, August 1996. http://csat.au.af.mil/2025/volume3/vol3ch02.pdf (accessed 29 December 2012).

Prisco, Nicholas E. “The Criticality of Cyber Defense to Operational Commanders.” Paper submitted to Naval War College, May 4, 2012. http://www.hsdl.org/?view&did=726655 (accessed 24 April 2013).

Purdy, Andy, Jr. “Forging a National Cyber Security Strategy.” *SC Magazine.com*, Mar 6, 2006. http://www.scmagazine.com/forging-a-national-cyber-security-strategy/article/33057/ (accessed 24 April 2013).

Quinter, Jason. “Joint Command and Control of Cyber Operations: The Joint Force Cyber Component Commander (JFCCC).” Research paper submitted to Naval War College, May 4, 2012. http://www.dtic.mil/dtic/tr/fulltext/u2/a564068.pdf (accessed 24 April 2013).

Rattray, Gregory. *Strategic Warfare in Cyberspace.* Cambridge, MA: Massachusetts Institute of Technology, 2001. http://books.google.com/books?hl=en&lr=&id=lVbQ4AxfYaMC&oi=fnd&pg=PP1&dq=Strategic+Warfare+in+Cyberspace&ots=OGA8sGQLiC&sig=Z-QOrM5FTcHxWbkLKE-LkiPTAzk#v=onepage&q=Strategic%20Warfare%20in%20Cyberspace&f=false (accessed 12 September 2012).

Reister, Brett. “Cyberspace: Regional and Global Perspectives.” Strategy research project, US Army War College, 2012. http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA561780 (accessed 24 April 2013).

Rid, Thomas. “Think Again: Cyberwar.” *Foreign Policy.com*, March/April 2012. http://www.foreignpolicy.com/articles/2012/02/27/cyberwar (accessed 24 April 2013).

Rosenzweig, Paul. *The Alarming Trend of Cybersecurity Breaches and Failures in the US Government*. Washington DC: The Heritage Foundation, May 24, 2012.

http://www.heritage.org/research/reports/2012/05/the-alarming-trend-of-cybersecurity-breaches-and-failures-in-the-us-government (accessed 24 April 2013).

Rutkowski, A. M. “Lessons from the First Great Cyberwar Era.” *Info* 12, no. 1 (2010): 5-9. http://cs.brown.edu/courses/csci1950-p/sources/2010_Info_v12_n1_Cyberwar_Lessons_Rutkowski.pdf (accessed 24 April 2013).

Sapolsky, Harvey. "Advice for the SecDef." *Proceedings Magazine.com*, January 2009. http://www.usni.org/magazines/proceedings/2009-01/advice-secdef-or-what-you-wont-hear-brookings-se (accessed 2 September 2012).

Schmitt, Michael N., “International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed.” *Harvard International Law Journal Online* 13 (2012). http://www.harvardilj.org/2012/12/online-articles-online_54_schmitt/ (accessed 19 April 2013).

Shaud, John and Adam Lowther. “An Air Force Strategic Vision for 2020-2030.” *Strategic Studies Quarterly* (Spring 2011): 8-31. http://www.au.af.mil/au/ssq/2011/spring/shaud-lowther.pdf (accessed 12 September 2012).

Sisson, Joseph E. “Fleet Cyber Command/TENTH Fleet: Enabling Cyber Unity of Effort.” Research paper submitted to US Naval War College, March 2010. http://www.dtic.mil/dtic/tr/fulltext/u2/a525307.pdf (accessed 24 April 2013).

Spade, Jayson C. “Information as Power: China's Cyber Power and America's National Security.” Strategy research project, US Army War College, 2011. http://www.carlisle.army.mil/dime/documents/China%27s%20Cyber%20Power%20and%20America%27s%20National%20Security%20Web%20Version.pdf (accessed 24 April 2013).

Snoddy, David. “A Case for Principles of Cyberspace Operations.” Monograph, US Naval War College, 2010. http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA535577 (accessed 24 April 2013).

Strate, Lance. “The Varieties of Cyberspace: Problems in Definition and Delimitation.” *Western Journal of Communication* 63, no. 3 (Summer 1999): 382-412. http://www.forbes.com/sites/ richardstiennon/2012/06/04/operation-olympic-game-project-x-and-the-assault-on-the-it-security-industry/ (accessed 6 February 2013).

Steinnon, Richard. “Operation Olympic Games, Project X, and the Assault on the IT Security Industry.” *Forbes.com*, June 4, *2012*. http://www.forbes.com/sites/richardstiennon/2012/06/04/operation-olympic-game-project-x-and-the-assault-on-the-it-security-industry/ (accessed 24 April 2013).

Stephanopoulos, George. “House Intel Chair Mike Rogers Calls Chinese Cyber Attacks ‘Unprecedented’.” *ABC OTUS News*, February 24, 2013. http://news.yahoo.com/house-intel-chair-mike-rogers-calls-chinese-cyber-180030656--abc-news-politics.html (accessed 25 February 2013).

Sun-Tzu. *The Art of War*. Translated by Ralph Sawyer. Boulder: Basic Books, 1994.

Thomas, Timothy. *Recasting the Red Star: Russia Forges Tradition and Technology through Toughness.* Fort Leavenworth: Foreign Military Studies Office, 2011.

Toffler, Alvin, and Heidi Toffler. *War and Anti-War.* New York: Warner Books, 1993.

U.S. Congress. House. Armed Services Committee. *Joint Chiefs of Staff Reorganization Act of 1985*. 99th Cong., 1st sess., 1985. Rep 99-375. https://digitalndulibrary.ndu.edu/cdm4/document.php?CISOROOT=/goldwater& CISOPTR=868&CISOSHOW=831 (accessed 9 April 2013).

U.S. Congress. House. Armed Services Committee. *Prepared Statement by Linda Robinson before the House Armed Services Committee, Subcommittee on Emerging Threats and Capabilities, Hearing on the Future of Special Operations Forces*. 112th Cong., 2nd sess., July 11, 2012. http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CDMQFjAA&url=http%3A%2F%2Fi.cfr.org%2Fcontent%2Fpublications%2Fattachments%2FL.RobinsonTestimony070912.pdf&ei=Nex3Ubm9H46w8QSz34DwBQ&usg=AFQjCNGNooyZRk_a8DY47epbIKzmoUe8_A&bvm=bv.45580626,d.eWU (accessed 24 April 2013).

U.S. Congress. House. Armed Services Committee. *Statement by Lieutenant General Rhett Hernandez Commanding General US Army Cyber Command/2nd Army before the emerging threats and capabilities of the house armed services committee on 25 July 2012*. http://armedservices.house. gov/index.cfm/hearings-display?ContentRecord_id=c0de6683-61a9-4b83-b443-8a8c45ff5009&Statement_id=7fc85bab-d453-4e30-947e-03bb1a48f5c9&ContentType_id=14f995b9-dfa5-407a-9d35-56cc7152a7ed&Group_id=41030bc2-0d05-4138-841f-90b0fbaa0f88&MonthDisplay=7&YearDisplay=2012 (accessed 12 September 2012).

U.S. Congress. House. Armed Services Committee. *Statement by Teresa M. Takai Department of Defense Chief Information Officer before The House Armed Services Committee Subcommittee On Emerging Threats and Capabilities on Fiscal Year 2013 Budget Request for Information Technology and Cyber Operations Programs.* March 20, 2012. http://armedservices.house.gov/index.cfm/files/serve?File_id=d6d557bc-a941-49e0-996a-d29cf376fb0d (accessed 6 April 2013).

U.S. Congress. House. Armed Services Committee. *Statement of Christopher J. Lamb Distinguished Research Fellow, Center for Strategic Research, Institute for National Strategic Studies, National Defense University On "The Future of US Special Operations Forces" before the Subcommittee on Emerging Threats and Capabilities*. July 11, 2012. http://armedservices.house.gov/index.cfm/hearings-display?ContentRecord_id=cbdaee80-36b1-4829-9d22-92089d55f978&ContentType_id=14f995b9-dfa5-407a-9d35-56cc7152a7ed&Group_id=64562e79-731a-4ac6-aab0-7bd8d1b7e890 (accessed 24 April 2013).

U.S. Congress. House. Armed Services Committee. *Statement of MGEN Suzanne M. Vautrinot Commander Air Forces Cyber 25 July 2012.* http://armedservices.house.gov/index.cfm/hearings-display?ContentRecord_id=c0de6683-61a9-4b83-b443-8a8c45ff5009&Statement_id=99f81c1d-b026-455e-b58d-

3288a8c57a12&ContentType_id=14f995b9-dfa5-407a-9d35-56cc7152a7ed
&Group_id=41030bc2-0d05-4138-841f-
90b0fbaa0f88&MonthDisplay=7&YearDisplay=2012 (accessed 12 September 2012).

U.S. Congress. House. Armed Services Committee. *Statement of VADM Michael S. Rogers Commander, United States Fleet Cyber Command before the emerging threats and capabilities of the house armed services committee on 25 July 2012.* http://armedservices.house.gov/ index.cfm/hearings-display?ContentRecord_id=c0de6683-61a9-4b83-b443-8a8c45ff5009 &Statement_id=7fc85bab-d453-4e30-947e-03bb1a48f5c9&ContentType_id=14f995b9-dfa5-407a-9d35-56cc7152a7ed&Group_id=41030bc2-0d05-4138-841f-90b0fbaa0f88& MonthDisplay=7&YearDisplay=2012 (accessed 12 September 2012).

U.S. Congress. Senate. *Statement of Stewart A. Baker, Partner Steptoe and Johnson LLP Before the Committee on Homeland Security and Governmental Affairs April 28, 2009.* http://www.hsgac.senate.gov/download/042809baker (accessed 12 September 2012).

U.S. Congress. Senate. Armed Services Committee. "*Oversight: US Strategic Command and US Cyber Command."* Webcast video of hearings held March 12, 2013. http://www.armed-services.senate.gov/hearings/event.cfm?eventid=0daf354e2970a9db3a6d0023abe58a27 (accessed 16 March 2013).

U.S. Congress. Senate. Armed Services Committee, Subcommittee on Emerging Threats and Capabilities. *Statement Testimony: the Honorable Zachary J. Lemnios Assistant Secretary of Defense for Research and Engineering Mar 20, 2012.* http://www.acq.osd.mil/chieftechnologist/.../ASDRE_Testimony_2011.pdf (accessed 12 September 2012).

U.S. Department of the Air Force. *2010 Combat Air Force Strategic Plan. SECURING THE HIGH GROUND: Agile Combat Power*. Washington DC: Department of the Air Force, 2010. http://www.acc.af.mil/shared/media/ document/AFD-100915-011.pdf (accessed 16 March 2013).

U.S. Department of the Air Force. *Air Force Doctrine Document 3-12, CYBERSPACE OPERATIONS.* LeMay Center/DD, 2010. http://www.e-publishing.af.mil/shared/media/ epubs/afdd3-12.pdf (accessed 12 September 2012).

U.S. Department of the Air Force. *Air Force Policy Directive 10-17, Cyberspace Operations.* www.e-publishing.af.mil, 31 July 2012. http://www.fas.org/irp/doddir/usaf/afpd10-17.pdf (accessed 24 April 2013).

U.S. Department of Defense. *2002 Year in Review.* Washington DC: Department of Defense, 2002. http://www.dtic.mil/docs/citations/ ADA475302 (accessed 28 December 2012).

U.S. Department of Defense. *Department of Defense Strategy for Operating in Cyberspace, July 2011.* Washington DC: Department of Defense, 2011. http://www.defense.gov/news/ d20110714cyber.pdf (accessed 15 February 2013).

U.S. Department of Defense. *Dictionary of Military and Associated Terms. 8 Nov 2010 as amended through 15 Nov 2012.* Washington DC: Department of Defense, 2012. http://ra.defense.gov/documents/rtm/jp1_02.pdf (accessed 29 January 2013).

U.S. Department of Defense. *Overview, Fiscal Year 2013 Budget Request.* Office of the Under Secretary of Defense (Comptroller) / Chief Financial Officer, February 2012. http://comptroller.defense.gov/defbudget/fy2013/FY2013_Budget_Request_Overview_Book.pdf (accessed 29 January 2013).

U.S. Department of Defense, *The Budget for Fiscal Year 2013.* Washington DC: Department of Defense, 2012. http://www.whitehouse.gov/sites/default/files/omb/budget/fy2013/assets/defense.pdf (accessed 6 Apr 2013).

U.S. Department of Defense. Defense Information Systems Agency. *Campaign Plan 2011-2012*. http://www.disa.mil/About/Our-Campaign-Plan (accessed 12 September 2012).

U.S. Department of Defense. Defense Information Systems Agency. *Strategic Plan 2013-2018 Version 1*. http://www.disa.mil/About/~/media/Files/DISA/About/Strategic-Plan.pdf (accessed 6 April 2013).

U.S. Department of Defense. *Sustaining US Global Leadership: Priorities for 21st Century Defense, January 2012.* http://www.defense.gov/news/Defense_Strategic_Guidance.pdf (accessed 12 September 2012).

U.S. Department of Defense. *Defense Budget Priorities and Choices, January 2012.* http://www.defense.gov/news/Defense_Budget_Priorities.pdf (accessed 12 September 2012).

U.S. Department of Defense and US Department of Homeland Security. *Memorandum of Agreement Between the Department of Homeland Security and the Department of Defense Regarding Cybersecurity.* http://www.dhs.gov/xlibrary/assets/20101013-dod-dhs-cyber-moa.pdf (accessed 12 September 2012).

U.S. Director of National Intelligence. *The National Intelligence Strategy of the United States of America, August 2009.* Washington DC: Government Printing Office, 2009.

U.S. Government Accountability Office. *Testimony Before the Subcommittee on Oversight, Investigations, and Management, Committee on Homeland Security, House of Representatives; Cybersecurity: Threats Impacting the Nation, Statement of Gregory C. Wilhusen, Director Information Security Issues*. Washington DC: Government Accountability Office, Apr 24, 2012. http://www.gao.gov/assets/600/590367.pdf (accessed 30 December 2012).

U.S. Government Accountability Office. *Defense Department Cyber Efforts: DoD Faces Challenges in its Cyber Activities, Report to Congressional Requesters.* Washington DC: Government Accountability Office, July, 2011. http://www.gao.gov/products/GAO-11-75 (accessed 30 December 2012).

U.S. Government Accountability Office. *Defense Department Cyber Efforts: More Detailed Guidance Needed to Ensure Military Services Develop Appropriate Cyberspace Capabilities*. Washington DC: Government Accountability Office, May 2011. http://cryptome.org/0004/gao-11-421.pdf (accessed 3 April 2013).

U.S. President. Executive Order. "Presidential Decision Directive/NSC-63." Washington DC, May 22, 1998. http://www.fas.org/irp/offdocs/pdd/pdd-63.htm (accessed 25 November 2012).

Vautrinot, Suzanne M. "Sharing the Cyber Journey." *Strategic Studies Quarterly* 6, no. 3 (Fall 2012): 71-88. http://www.au.af.mil/au/ssq/2012/fall/fall12.pdf (accessed 7 April 2013).

Wei-cheng, Vincent and Gwendolyn Stamper. "Asymmetric war? Implications for China's information warfare strategies." *American Asian Review* 20, no. 4 (Winter 2002): 167-207. http://web.ebscohost.com/ehost/pdfviewer/pdfviewer?sid=496e0356-c823-4836-836e-104d7d55db6d%40sessionmgr104&vid=2&hid=125 (accessed 24 April 2013).

Wenzel, Frank. "Should the Department of Defense establish a Unified US Logistics Command?" Monograph, United States Army Command and General Staff College, 2008. http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA494098 (accessed 24 April 2013).

Wilhusen, Gregory C. *Cybersecurity: Threats Impacting the Nation.* U.S. Government Accountability Office, Apr 24, 2012. http://www.gao.gov/assets/ 600/590367.pdf (accessed 30 December 2012).

Wolk, Herman S. *Toward Independence, The Emergence of the US Air Force 1945-1947*. Washington DC: Government Printing Office, October 1996.